ViPNet VPN 4.4

Benutzerhandbuch





Ziel und Zweck

Dieses Handbuch beschreibt die Installation und Konfiguration von ViPNet Produkten. Für die neuesten Informationen und Hinweise zum aktuellen Software-Release sollten Sie in jedem Fall zusätzlich unsere Release Notes lesen – insbesondere, wenn Sie ein Software-Upgrade zu einem höheren Release-Stand durchführen. Die aktuellsten Release Notes sind immer zu finden unter http://www.infotecs.de

Haftung

Der Inhalt dieses Handbuchs wurde mit größter Sorgfalt erarbeitet. Die Angaben in Ihrem Handbuch gelten jedoch nicht als Zusicherung von Eigenschaften Ihres Produkts. Der Hersteller haftet nur im Umfang seiner Verkaufs- und Lieferbedingungen und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen.

Die Informationen in diesem Handbuch können ohne Ankündigung geändert werden. Zusätzliche Informationen, sowie Änderungen und Release Notes für ViPNet Produkte finden Sie unter http://www.infotecs.de. Der Hersteller übernimmt keine Verantwortung für Datenverlust und Schäden, die durch den unsachgemäßen Betrieb des Produkts entstanden sind.

Version: 00121-04 34 01 DEU

Wie Sie Infotecs erreichen

Infotecs GmbH

Oberwallstr. 24

10117 Berlin

Deutschland

Tel.: +49 (0) 30 206 43 66 0

Fax: +49 (0) 30 206 43 66 66

WWW: http://www.infotecs.de

E-Mail: support@infotecs.de

Inhaltsübersicht

Inhalt



Einführung

Über dieses Dokument

Zielgruppe

Dieses Benutzerhandbuch richtet sich in erster Linie an Netzwerkadministratoren, in deren Verantwortungsbereich der Aufbau und die Konfiguration des firmeninternen ViPNet Netzwerks fällt. Es werden keine tiefen Kenntnisse im Bereich der IT-Technologie vorausgesetzt, Grundkenntnisse über Netzwerktechnologien, IP-Protokolle, Firewalls, Verschlüsselung und Netzwerksicherheit sollten jedoch vorhanden sein.

Das Handbuch soll Ihnen helfen, ein leistungsfähiges und sicheres VPN-Netzwerk (Virtual Private Network) einzurichten, ohne sich dabei in die technischen Details vertiefen oder sich zusätzlich fortbilden zu müssen. Alle Informationen zur Einrichtung, Administration und Fehlerbehebung im VPN-Netzwerk, das auf Basis der ViPNet Technologie eingerichtet wurde, sind in diesem Dokument enthalten.

Verwendete Konventionen

Weiter unten sind Konventionen aufgeführt, die im gegebenen Dokument zur Kennzeichnung wichtiger Informationen verwendet werden.

Tabelle 1. Symbole, die für Anmerkungen benutzt werden

Symbol	Beschreibung
	Achtung! Dieses Symbol weist auf einen Vorgang hin, der für die Daten- oder Systemsicherheit wichtig ist.
	Hinweis. Dieses Symbol weist auf einen Vorgang hin, der es Ihnen ermöglicht, Ihre Arbeit mit dem Programm zu optimieren.
	Tipp. Dieses Symbol weist auf zusätzliche Informationen hin.

Tabelle 2. Notationen, die zur Kennzeichnung von Informationen im Text verwendet werden

Notation	Beschreibung
Name	Namen von Elementen der Benutzeroberfläche. Beispiele: Fensterüberschriften, Feldnamen, Schaltflächen oder Tasten.
Taste+Taste	Tastenkombinationen. Zum Betätigen von Tastenkombinationen sollte zunächst die erste Taste gedrückt und dann, ohne die erste Taste zu lösen, die zweite Taste gedrückt werden.

Notation	Beschreibung
Menü > **Untermenü** > **Befehl**	Hierarchische Abfolge von Elementen. Beispiele: Menüeinträge oder Bereiche der Navigationsleiste.
`Code`	Dateinamen, Pfade, Fragmente von Textdateien und Codeabschnitten oder Befehle, die aus der Befehlszeile ausgeführt werden.

Über ViPNet VPN

Moderne Unternehmen sehen sich immer häufiger mit Fragen der Informationssicherheit in lokalen und globalen Netzwerken konfrontiert. Lokale, entfernte und mobile Benutzer brauchen genauso wie räumlich entfernte Niederlassungen zuverlässige, abgesicherte Systeme für ihre Kommunikation.

Das Programmpaket ViPNet VPN ermöglicht es, ein virtuelles privates Netzwerk (VPN) mit hohen Sicherheitsstandards einzurichten, ohne dabei die bestehende physikalische Netzwerkstruktur zu ändern oder ihre Leistungskapazität zu beeinträchtigen. In ViPNet VPN sind eine Reihe von Tools integriert, mit deren Hilfe die Benutzer einfach und sicher im Netzwerk kommunizieren können. Die Installation von ViPNet VPN wird schnell und unkompliziert durchgeführt.

Der Vorteil der ViPNet Technologie besteht darin, dass die Integrität aller übertragenen Daten gewährleistet wird und das Netzwerk vor externen und internen Angriffen geschützt wird. Diese Sicherheitsmaßnahmen werden durch die Installation verschiedener Software-Module auf alle Computer im Netzwerk (sowohl auf Arbeitsstationen als auch auf Server) erfüllt. Die ViPNet Software kontrolliert den gesamten TCP/IP-Datenverkehr, indem sie diesen entsprechend den festgelegten Sicherheitsrichtlinien filtert und verschlüsselt. Wenn zwei Computer mit installierter ViPNet Software, unabhängig davon, ob sie sich innerhalb oder außerhalb des lokalen Netzwerks befinden, miteinander eine Verbindung aufbauen, wird diese Verbindung verschlüsselt und sofort von außen durch einen sicheren Tunnel abgeschottet. Die getunnelte Verbindung wird über bestehende Internet/Intranet-Kanäle aufgebaut und mit sicheren Verschlüsselungsalgorithmen verschlüsselt. Diese Verbindung kann nicht unterbrochen oder abgefangen werden. Ein ViPNet Netzwerk stellt somit ein Zusammenschluss von Computern dar, die miteinander über das Internet verbunden sind und zwischen denen eine verschlüsselte Kommunikation stattfindet.

Mit dem Begriff „Netzwerk" sind in diesem Zusammenhang übergreifend alle TCP/IP-Kommunikationsnetze gemeint, einschließlich Internet, LAN und anderer Netzwerkarten – unabhängig von Übertragungsmedien, Bandbreiten und Anschlusstypen. Die ViPNet Technologie ist mit allen gängigen Zugangsarten zum Internet kompatibel (xDSL, ISDN, GPRS, UMTS, Wi-Fi usw.).

Klassische VPN-Lösungen sind normalerweise darauf ausgerichtet, den Traffic zwischen zwei lokalen Netzwerken oder zwischen dem lokalen Netzwerk und den entfernten (mobilen) Benutzern zu schützen. Bedrohungsquellen innerhalb des lokalen Netzwerks werden häufig unterschätzt. Die ViPNet Technologie gewährleistet den Aufbau unmittelbarer, abgesicherter Client-to-Client-Verbindungen. Außerdem sind alle ViPNet VPN-Komponenten mit einer Firewall ausgestattet, was den Kommunikationsschutz sowohl zwischen entfernten Netzwerken als auch innerhalb des lokalen Netzwerkes gewährleistet.

Neue Möglichkeiten der Version 4.4

In diesem Abschnitt wird eine kurze Übersicht der Änderungen und neuen Möglichkeiten der Version 4.4 geboten.

Informationen über Änderungen in den vorherigen Versionen von ViPNet Network Manager sind im Anhang Versionsgeschichte von ViPNet VPN (auf S. 341) geschrieben.

- **Zentralisierte Lizenzverteilung**

  Zusätzliche ViPNet Software und Funktionen konnten zuvor separat für jeden Knoten im Programm ViPNet Network Manager in der Registerkarte **Schlüssel** festgelegt werden. Jetzt können die Lizenzeinschränkungen für die Verwendung von zusätzlichen ViPNet Komponenten zentralisiert für alle benötigten Knoten im Bereich **Eigenes Netzwerk** in der Registerkarte **Allgemeines** verteilt werden (s. Verwendung zusätzlicher ViPNet Komponenten auf S. 123).

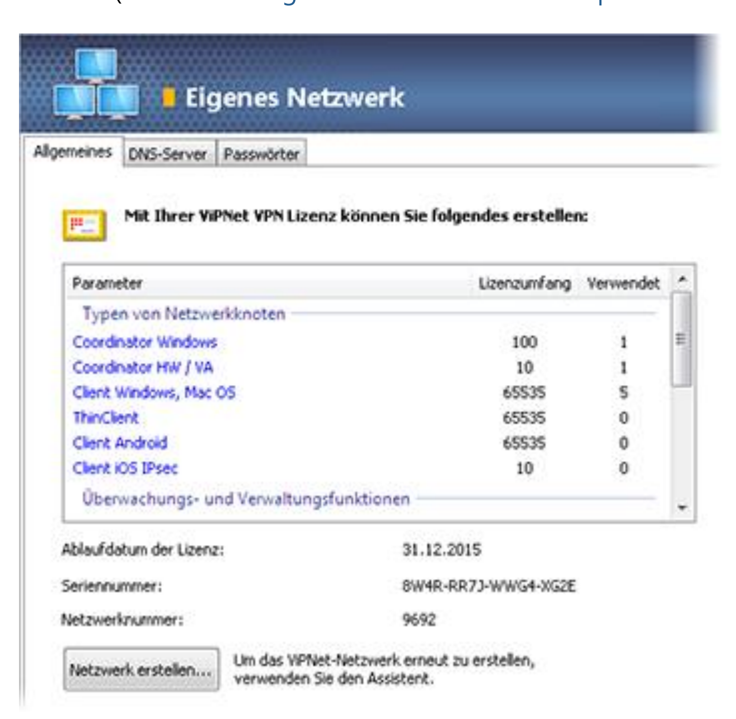


Abbildung 1. Lizenzeinschränkungen für zusätzliche ViPNet Komponenten

  In der Registerkarte **Schlüssel** kann die Verwendung der Komponenten ViPNet Business Mail, ViPNet SafeDisk-V und ViPNet Failover nicht mehr erlaubt werden.

- **Unterstützung von ViPNet Connect**

  Im Programm ViPNet Network Manager kann jetzt die Verwendung der Software ViPNet Connect auf den Clients ViPNet Client für Windows, ViPNet Client for Android, ViPNet Client für Mac OS X erlaubt werden. Die Benutzer des ViPNet Netzwerkes können mit Hilfe dieses Programms über den geschützten VPN-Kanal einander anrufen (s. ViPNet Connect auf S. 41). In der ViPNet VPN Testversion wurde auch die Möglichkeit, das Programm ViPNet Connect auf zehn Clients zu verwenden, hinzugefügt.

- **Vereinfachte Konfiguration der Firewall für Clients**

Die Verbindung der Clients über eine Firewall zu einem externen Netzwerk wird jetzt automatisch durch das Programm ViPNet Network Manager konfiguriert. Die Einstellungen hängen dabei vom Client-Typen ab:

- Für alle Clients wird die Verbindung über eine Firewall mit dynamischem NAT konfiguriert.
- Für Clients ViPNet Client for Android und ViPNet Client für Mac OS X wird zusätzlich die Weiterleitung des Datenverkehrs über ihren Coordinator konfiguriert.

Diese Änderungen hängen damit zusammen, dass im ViPNet Netzwerk neue Technologien für Verbindungen zwischen den Knoten verwendet werden. Jetzt wird nicht unterstützt, dass sich Clients in anderen Modi über eine Firewall zu einem externen Netzwerk verbinden.

Wird das Programm ViPNet Network Manager auf die Version 4.4 aktualisiert, werden abweichende Verbindungseinstellungen über eine Firewall für alle Clients gemäß den neuen Anforderungen angepasst.

Entsprechende Änderungen sind bereits in der Oberfläche des ViPNet Network Manager vorgenommen, d.h. die Registerkarte **Firewall** für Clients wurde gelöscht.

- **Unterstützung der Software ViPNet Client und ViPNet Coordinator für Windows der Version 4.3**

  Das Programm ViPNet Network Manager unterstützte zuvor ViPNet Client für Windows und ViPNet Coordinator für Windows der Version 4.2. Jetzt wird die Software der Version 4.3 verwendet.

  Informationen über neue Möglichkeiten der Software ViPNet Client für Windows und ViPNet Coordinator für Windows finden Sie im Dokument „Neue Möglichkeiten von ViPNet VPN 4.x. Anhang zum ViPNet VPN Benutzerhandbuch".

- **Unterstützung neuer Ausführungen von ViPNet Coordinator HW**

  Wenn es eine entsprechende Lizenz vorliegt, können Sie jetzt die Appliances ViPNet Coordinator HW1000 und HW2000 in Ihrem ViPNet Netzwerk verwenden. In diesen Ausführungen werden Server mit hoher Leistungskapazität als Hardwareplattform verwendet (s. Modifikationen von ViPNet Coordinator HW auf S. 34).

  Es wurden auch Änderungen in den zuvor unterstützten Ausführungen vorgenommen: Die Ausführung HW100 Andvanced wurde in HW100 umbenannt, die ehemalige Ausführung HW100 wird vorübergehend nicht unterstützt.

- **Auswahl der Knoten und Speicherung der Schlüssel**

  Früher wurde die Massenspeicherung der Schlüsseldistributionen für alle Netzwerkknoten gleichzeitig durchgeführt. In der neuen Programmversion besteht die Möglichkeit, bestimmte Knoten auszuwählen, für welche die Schlüssel dann erstellt werden. Nun können Sie die Schüsseldistributionen massenweise nur für neue Knoten (diese sind in der Liste standardmäßig ausgewählt) erstellen bzw. nur Knoten berücksichtigen, an die der Versand der Schlüssel über das ViPNet Netzwerk aus irgendwelchen Gründen nicht möglich ist.

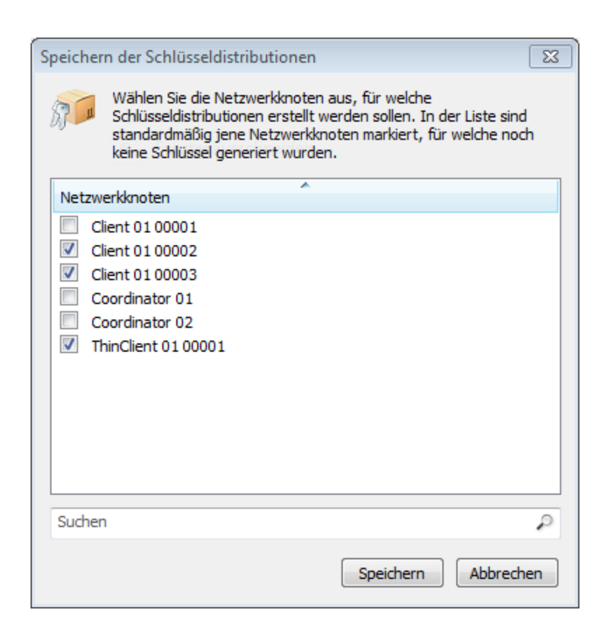


Abbildung 2. Auswahl der Knoten zum Speichern der Schlüssel

- **Änderungen in der IPsec-Konfiguration für Netzwerkknoten ViPNet Coordinator HW/VA**

  In früheren Versionen konnte die IP-Adresse bzw. der DNS-Name für Netzwerkknoten ViPNet Coordinator HW/VA, die als IPsec-Gateways im Einsatz sind, nur für Verbindungen mit Smartphone-Clients festgelegt werden. Nun kann die Adresse auch bei einer IPsec-Verbindung mit dem betroffenen Netzwerk definiert werden. Dadurch können Netzwerkknoten ViPNet Coordinator HW/VA, die sich hinter einer Firewall mit NAT befinden, als IPsec-Gateways für Verbindungen zu anderen Netzwerken eingesetzt werden.

- **Massenlöschung der Netzwerkknoten**

  Wenn Sie zuvor mehrere Knoten aus dem ViPNet Netzwerk löschen wollten, dann mussten Sie die Knoten in der Navigationsleiste von ViPNet Network Manager der Reihe nach einzeln markieren. Nun können Sie mehrere Knoten gleichzeitig auswählen, wodurch die Netzwerkstruktur schneller und einfacher geändert werden kann.

Systemanforderungen

Die Software ViPNet VPN kann innerhalb eines Netzwerks installiert werden, das mit Hilfe beliebiger drahtgebundener oder drahtloser Verbindungskanäle aufgebaut wurde (Ethernet, DSL, Wi-Fi, 3G u. s. w.).

In diesem Dokument werden die wichtigsten Komponenten von ViPNet VPN beschrieben: die Programme ViPNet Network Manager, ViPNet Coordinator und ViPNet Client für Windows. Des Weiteren können Sie den Coordinator ViPNet Coordinator HW/VA, den Client ViPNet Client for Mac OS und andere zusätzliche Komponenten in Ihrem Netzwerk verwenden (s. Die Komponenten von ViPNet VPN auf S. 27).

Die Installation von ViPNet VPN erfolgt mit Hilfe eines Installationsprogramms. Folgende Hardware-Mindestanforderungen müssen erfüllt sein, um die einzelnen Komponenten von ViPNet VPN zu installieren.

ViPNet Network Manager

Die Software ViPNet Network Manager sollte auf einem Netzwerkknoten installiert werden, der als Arbeitsstation des ViPNet Administrators vorgesehen ist. Weil die vom Programm ViPNet Network Manager erstellten Dateien vertrauliche Daten enthalten, sollte nur der Administrator über einen Zugang zu diesem Computer verfügen.

Folgende Hardware-Mindestanforderungen sollten für die Installation von ViPNet Network Manager erfüllt sein:

- Prozessor: ein Intel Core 2 Duo oder ein anderer x86-kompatible Prozessoren mit mindestens zwei Kernen wird empfohlen.
- Arbeitsspeicher: mindestens 1 GB RAM (4 GB ist empfehlenswert).
- Freier Festplattenspeicher: mindestens 500 MB.
- Netzwerkadapter oder Modem.
- Betriebssystem: Microsoft Windows Vista (32/64-Bit), Server 2008 (32/64-Bit), Windows 7 (32/64-Bit), Server 2008 R2 (64-Bit), Small Business Server 2008 (64-Bit), Small Business Server 2011 (64-Bit), Windows 8 (32/64-Bit), Windows 8.1 (32/64-Bit), Windows Server 2012 R2 (64-Bit), Windows 10 Technical Preview (32/64-Bit).

  Im Betriebssystem sollte das neueste Updatepaket installiert sein.
- Falls Internet Explorer verwendet wird: Version 6.0 oder höher.
- Für den Versand von automatisch erstellten Nachrichten über die Arbeit von ViPNet Anwendungen und die Softwareumgebung an den technischen Support von „Infotecs" eignet sich jeder beliebige E-Mail-Client.

Für die ordnungsgemäße Installation und Einsatz von ViPNet Network Manager wird zusätzliche Software benötigt:

- Microsoft SQL Server 2008 R2 Express Edition. Diese Software ist im Lieferumfang von ViPNet VPN enthalten und wird automatisch mit dem Programm ViPNet Network Manager installiert.
- Microsoft Windows Installer 4.5 bei Verwendung der Betriebssysteme Microsoft Windows Server 2008 (32-Bit), Small Business Server 2003 (32-Bit), Small Business Server 2008 (64-Bit).
- Microsoft .NET Framework 3.5 (SP1) bei Verwendung der Betriebssysteme Microsoft Windows Server 2008 (32-Bit), Small Business Server 2003 (32-Bit), Small Business Server 2008 (64-Bit).



Hinweis. Sie können diese Software kostenlos von der Webseite der Firma Microsoft herunterladen:

- Microsoft Windows Installer 4.5 http://www.microsoft.com/de-de/download/details.aspx?id=8483.
- Microsoft .NET Framework 3.5 http://www.microsoft.com/de-de/download/details.aspx?id=21.

ViPNet Coordinator

Folgende Mindestanforderungen müssen für die Installation von ViPNet Coordinator erfüllt sein:

- Prozessor: ein Intel Core 2 Duo oder ein anderer x86-kompatible Prozessoren mit mindestens zwei Kernen wird empfohlen.
- Das empfohlene Arbeitsspeichervolumen ist abhängig von der Anzahl der Clients, die dem Coordinator zugeordnet sind:

Anzahl der Clients	RAM
Bis 1000	mindestens 1 GB
Bis 5000	mindestens 2 GB

- Freier Festplattenspeicher: mindestens 1 GB.
- Netzwerkadapter oder Modem. Die Anzahl der Netzwerkadapter hängt von den Anforderungen an die Funktionalität des Coordinators ab.
- Betriebssystem: Windows XP (32-Bit), Server 2003 (32-Bit), Vista (32/64-Bit), Server 2008 (32/64-Bit), Windows 7 (32/64-Bit), Windows 8 (32/64-Bit), Windows 8.1 (32/64-Bit), Server 2012 (64-Bit), Server 2012 R2 (64-Bit).

  Im Betriebssystem sollte das neueste Updatepaket installiert sein.
- Bei Verwendung früherer Windows-Versionen als Windows 8 sollte auf dem Computer das kumulative Zeitzonenupdate KB2570791 installiert werden.

- Falls Internet Explorer verwendet wird: Version 6.0 oder höher.



Hinweis. Damit die Funktionsfähigkeit von ViPNet Coordinator gewährleistet werden kann, sollten auf dem Computer keine weiteren Firewalls und softwarebasierten NAT-Lösungen anderer Hersteller installiert sein.

ViPNet Client

Das Programm ViPNet Client (Windows) sollte auf allen Benutzercomputern installiert werden.

Folgende Anforderungen müssen für die Installation von ViPNet Client erfüllt sein:

- Prozessor: ein Intel Core 2 Duo oder ein anderer x86-kompatible Prozessoren mit mindestens zwei Kernen wird empfohlen.
- Arbeitsspeicher: mindestens 1 GB RAM.
- Freier Festplattenspeicher: mindestens 150 MB (250 MB sind empfehlenswert).
- Netzwerkadapter oder Modem.
- Betriebssystem: Windows XP (32-Bit), Server 2003 (32-Bit), Vista (32/64-Bit), Server 2008 (32/64-Bit), Server 2008 R2 (64-Bit), Windows 7 (32/64-Bit), Windows 8 (32/64-Bit), Windows 8.1 (32/64-Bit), Server 2012 (64-Bit), Server 2012 R2 (64-Bit).

  Im Betriebssystem sollte das neueste Updatepaket installiert sein.
- Bei Verwendung früherer Windows-Versionen als Windows 8 sollte auf dem Computer das kumulative Zeitzonenupdate KB2570791 installiert werden.
- Falls Internet Explorer verwendet wird: Version 6.0 oder höher.



Hinweis. Auf dem Computer sollten keine weiteren Firewalls installiert sein.

Lieferumfang

Die archivierte Installationsdatei für ViPNet VPN kann von der Internetseite der Infotecs GmbH heruntergeladen werden http://www.infotecs.de/products/.

Das Installationspaket ViPNet VPN beinhaltet:

- Das einheitliche Installationsprogramm von ViPNet VPN für die Installation folgender Komponenten:
  - ViPNet Network Manager mitsamt zusätzlicher Software Microsoft SQL Server 2008 R2 Express Edition.
  - ViPNet Client (Windows).
  - ViPNet Coordinator.



Hinweis. Mit Hilfe der einheitlichen Installationsdatei kann auch eine Demoversion von ViPNet VPN installiert werden, die einer Reihe funktioneller Einschränkungen unterliegt (s. Einschränkungen der kostenlosen Version auf S. 47). Zum Aufheben dieser Einschränkungen sollte das Programm ViPNet Network Manager registriert werden (s. Registrierung von ViPNet Network Manager auf S. 70).

- Handbücher im PDF-Format, u. a.:
  - ViPNet VPN. Benutzerhandbuch.
  - ViPNet VPN. Schnellstart.
  - Aufbauszenarien ViPNet VPN. Anhang zum ViPNet VPN Benutzerhandbuch.
  - Gemeinsame Verwendung von ViPNet VPN und Cisco IP-Telefonie. Anhang zum ViPNet VPN Benutzerhandbuch.
  - Gängige Szenarien der Administration von ViPNet VPN. Anhang zum Benutzerhandbuch.
  - Die Technologie von ViPNet. Allgemeine Informationen.
  - Grundsätze beim Aufbau von Verbindungen im ViPNet Netzwerk. Allgemeine Informationen.
  - Neue Möglichkeiten von ViPNet VPN 4.x. Anhang zum ViPNet VPN Benutzerhandbuch

Kontakt

FAQ und andere Hilfsinformation

Informationen über ViPNet-Produkte und Lösungen, gängige Fragen und andere nützliche Hinweise sind auf der Webseite von „InfoTeCS“ zusammengefasst. Unter den aufgeführten Links können Sie zahlreiche Antworten auf mögliche während des Produktbetriebs auftretenden Fragen finden.

- Allgemeine Geschäftsbedingungen http://www.infotecs.de/about/terms.php
- ViPNet-Lösungen im Überblick http://www.infotecs.de/solutions/
- Frequently Asked Questions http://www.infotecs.biz/doc_vipnet/DEU/index.htm#2_11572.htm
- ViPNet-Wissensdatenbank http://www.infotecs.biz/doc_vipnet/DEU/index.htm#1_main.htm

Kontakt

Bei Fragen zur Nutzung von ViPNet-Software sowie möglichen Wünschen und Anregungen nehmen Sie Kontakt mit den Mitarbeitern der Firma „InfoTeCS GmbH“ auf. Für die Lösung aufgetretener Problemfälle wenden Sie sich an den technischen Support.

- E-Mail: support@infotecs.de.
- Anfrage an den technischen Support via Internetseite http://infotecs.de/support/
- Support Hotline +49 (0) 30 206 43 66 22 (Tel.); +49 (0) 30 206 43 66 66 (Fax).



Allgemeines

Die Komponenten von ViPNet VPN

Das ViPNet VPN-Paket für den Aufbau von VPN-Netzwerken (s. Virtuelles Privates Netzwerk (VPN) auf S. 374) beinhaltet die folgenden Komponenten:

- Hauptkomponenten:
  - ViPNet Network Manager,
  - ViPNet Coordinator für Windows,
  - ViPNet Client für Windows.
- Zusätzliche Komponenten:
  - ViPNet Coordinator HW/VA,
  - ViPNet Client for Mac OS X,
  - ViPNet Client for Android,
  - ViPNet ThinClient,
  - ViPNet StateWatcher,
  - ViPNet Policy Manager,
  - ViPNet SafeDisk-V,
  - ViPNet Connect.



Hinweis. In diesem Dokument wird ausschließlich die Verwendung der Basiskomponenten beschrieben.

ViPNet Network Manager

Das Programm ViPNet Network Manager sollte auf einer eigens dafür vorgesehenen Arbeitsstation des ViPNet Netzwerkadministrators vor allen anderen Komponenten des ViPNet VPN-Pakets installiert werden.

ViPNet Network Manager erstellt die logische Struktur des ViPNet Netzwerks (d.h. die Verbindungen zwischen den Servern und den Benutzerarbeitsplätzen) und generiert die Schlüsseldistributionen und die Benutzerpasswörter für jeden Netzwerkknoten. Die Schlüsseldistributionen werden dazu verwendet, verschlüsselte Verbindungen aufzubauen, und sind für die Installation von ViPNet Coordinator und ViPNet Client auf den Netzwerkknoten erforderlich.

Damit der ViPNet Netzwerkadministrator Verbindungen zu anderen ViPNet Netzwerkknoten aufbauen und Schlüssel versenden kann, sollte auf dem Manager-Arbeitsplatz das Programm ViPNet Client oder ViPNet Coordinator installiert werden (im Programm ViPNet Network Manager wird der Netzwerkknoten, der als Manager-Arbeitsplatz eingesetzt wird, mit dem Symbol oder gekennzeichnet).

ViPNet Network Manager beinhaltet den Assistenten **ViPNet Netzwerk-Aufbau**, der den Benutzer beim Aufbau eines ViPNet Netzwerks Schritt für Schritt unterstützt. Dieser Assistent verfügt über eine benutzerfreundliche Schnittstelle und erleichtert die Installation des Netzwerks insbesondere beim ersten Mal.

ViPNet Network Manager bietet die Möglichkeit, Sicherungskopien von Netzwerkkonfigurationen zu erstellen sowie Remoteupdates der ViPNet Software auf den Netzwerkknoten durchführen.

Außerdem können mit Hilfe von ViPNet Network Manager Partnernetzwerk-Verbindungen vom eigenen Netzwerk zu anderen ViPNet Netzwerken eingerichtet werden. Zum Beispiel kann das Netzwerk einer Firmenzentrale mit dem Netzwerk einer Niederlassung verbunden werden. Dabei kann sich die Niederlassung in einem anderen Land oder auf einem anderen Kontinent befinden. Zwischen der Zentrale und der Filiale wird ein geschützter VPN-Kanal aufgebaut, über den die verschlüsselte Kommunikation ohne zusätzlichen Aufwand stattfindet. Es können beliebig viele Filialen mit eigenen ViPNet Netzwerken zu einem großen VPN-Netzwerk zusammengefasst werden.

Aud einen Computer mit der ViPNet Network Manager Software können Sie folgende zusätzliche Steuerungskomponenten installieren: das Softwaresystem zur Überwachung von geschützten Netzwerken ViPNet StateWatcher, das der Statusüberwachung von ViPNet Netzwerkknoten dient (s. Verwendung der Software ViPNet StateWatcher auf S. 120), und das Programm ViPNet Policy Manager für zentralisierte Verwaltung der Sicherheistrichtlinien von Netzwerkknoten (s. Verwendung der Software ViPNet Policy Manager auf S. 120).

ViPNet Coordinator für Windows

Die ViPNet Coordinator Software wird auf den Netzwerkknoten installiert, welche als Server im geschützten ViPNet Netzwerk agieren (s. Funktionen des Coordinators im ViPNet Netzwerk auf S. 239).

ViPNet Coordinator besteht aus folgenden Hauptkomponenten (s. Softwarekomponenten von ViPNet Client und ViPNet Coordinator für Windows auf S. 29):

- ViPNet Treiber – Kernel-Level Netzwerkschutztreiber (s. ViPNet Kryptotreiber auf S. 29).
- ViPNet Monitor (auf S. 30).
- ViPNet MFTP (auf S. 30).
- ViPNet Programmkontrolle (auf S. 31).

ViPNet Client für Windows

Die ViPNet Client-Software erfüllt die Funktionen eines VPN-Clients im ViPNet Netzwerk und schützt den Computer vor unerlaubten Zugriffen während der Arbeit in lokalen und globalen Netzwerken.

ViPNet Client-Software kann auf einem beliebigen Computer mit Betriebssystem Windows installiert werden, unabhängig davon, ob es sich um einen stationären, entfernten oder mobilen Computer oder Server handelt.

Die Software ViPNet Client umfasst die folgenden Komponenten (s. Softwarekomponenten von ViPNet Client und ViPNet Coordinator für Windows auf S. 29):

- ViPNet Treiber – Kernel-Level Netzwerkschutztreiber (s. ViPNet Kryptotreiber auf S. 29).
- ViPNet Monitor (auf S. 30).
- ViPNet MFTP (auf S. 30).
- ViPNet Business Mail (auf S. 30).



Hinweis. Das Programm ViPNet Business Mail kann erst dann auf den Client installiert werden, wenn die Verwendung des Programms auf dem betroffenen Knoten im Programm ViPNet Network Manager freigegeben wurde (s. Installation des Programms ViPNet Business Mail auf S. 229).

Softwarekomponenten von ViPNet Client und ViPNet Coordinator für Windows

ViPNet Kryptotreiber

ViPNet Kryptotreiber ist ein Low-Level-Netzwerkschutztreiber, der die Verschlüsselung und Filterung des IP-Traffics durchführt. Der ViPNet Treiber interagiert unmittelbar mit den Netzwerkadaptertreibern des Betriebssystems (ob nativ oder emuliert), was die Unabhängigkeit des Programms vom jeweiligen Betriebssystem und den undokumentierten Möglichkeiten darin gewährleistet. Der ViPNet Kryptotreiber fängt den gesamten eingehenden und ausgehenden IP-Datenverkehr auf einem Computer ab und kontrolliert diesen.

Zu den wichtigsten Funktionen des Kryptotreibers gehört die sichere Überwachung des IP-Traffics beim Hochfahren des Betriebssystems. Im Betriebssystem Windows wird für die Initialisierung des Neustarts nur ein Dienst verwendet. Die Initialisierung des ViPNet Kryptotreibers und der ViPNet Schlüssel findet vor der Benutzeranmeldung in Windows statt, d. h. noch vor der Initialisierung anderer Dienste und Treiber des Betriebssystems.

Der ViPNet-Kryptotreiber übernimmt somit als erster die Kontrolle über den TCP/IP-Stack. Zum Zeitpunkt der Initialisierung der Netzwerkadapter ist der Kryptotreiber bereits imstande, den Datenverkehr zu filtern und zu verschlüsseln. Dadurch werden gesicherte Verbindungen mit dem Domain Controller, die Kontrolle der Netzwerkaktivitäten aller Anwendungen auf dem Computer und die Blockierung aller unerwünschten eingehenden Pakete sichergestellt. Während des Bootvorgangs des Betriebssystems überprüft ViPNet Software eigene Prüfsummen, die die Integrität der Software, der Schlüsseldistributionen und aller Anwendungen mit Netzwerkaktivitäten gewährleisten.

Ausführliche Informationen über ViPNet-Kryptotreiber sehen Sie im Dokument „ViPNet Technologie. Allgemeine Informationen".

ViPNet MFTP

Als Bestandteil von ViPNet Client und ViPNet Coordinator erfüllt das MFTP-Modul die Funktion eines Kommunikationsservers, regelt das Empfangen und Versenden der Transportpakete und gewährleistet den Austausch von Dienst-, Adress- und Schlüsseldaten mit dem Programm ViPNet Network Manager, das auf dem Manager-Arbeitsplatz installiert ist.

Auf einem Client gewährleistet das MFTP-Modul den Austausch von Dienstpaketen, Business Mail-Nachrichten und sonstigen Dateien mit anderen ViPNet Netzwerkknoten.

Ausführliche Informationen über MFTP-Modul finden Sie im Abschnitt Transportmodul ViPNet MFTP (auf S. 318).

ViPNet Monitor

Zu den grundlegenden Funktionen des Programms ViPNet Monitor gehören die Möglichkeit der Konfiguration unterschiedlicher Parameter des ViPNet Treibers sowie das Aufzeichnen von Ereignissen, die im Zuge der Traffic-Verarbeitung durch den Treiber auftreten, in der Logdatei der registrierten IP-Pakete (s. Verwendung der Logdatei auf S. 324). Wenn ViPNet Monitor aus dem Hauptspeicher entladen wird, setzt der ViPNet Treiber seine Arbeit fort und sorgt für die Sicherheit des Computers. Bestimmte Daten über den IP-Traffic, der vom Treiber während der Inaktivität von ViPNet Monitor verarbeitet wurde, werden aber in der Logdatei nicht festgehalten (der ViPNet Treiber selbst kann nicht mehr als 10 000 Protokolleinträge speichern).

Auf dem Computer erfüllt ViPNet Monitor die folgenden Funktionen:

- Ermöglicht die Konfiguration der Parameter der integrierten Firewall auf dem Computer (s. Integrierte Firewall auf S. 269).
- Ermöglicht Bearbeitungsparameter der Anwendungsprotokolle zu verwenden (s. Bearbeitung der Anwendungsprotokolle auf S. 293).
- Stellt die Kommunikationsanwendungen für den verschlüsselten Nachrichtenaustausch, für die Durchführung von Chat-Konferenzen und für den sicheren Dateiaustausch zur Verfügung (s. Integrierte Kommunikationsmittel auf S. 31).

ViPNet Business Mail

„Business Mail" ist ein Bestandteil der Software ViPNet Client und dafür bestimmt, den verschlüsselten Versand von E-Mails zwischen den ViPNet Netzwerkbenutzern zu gewährleisten. Mit Hilfe von „Business Mail" können Nachrichten mit oder ohne Anhang versendet, Nachrichten und Anhänge verschlüsselt, E-Mails und angehängte Dateien mit einer elektronischen Signatur versehen werden. Die ein- und ausgehenden Nachrichten können nach definierten Richtlinien automatisch bearbeitet werden (Autoprocessing).

Der Netzwerkadministrator legt im Programm ViPNet Network Manager fest, dass das Programm ViPNet Business Mail auf ViPNet Clients für Windows verwendet werden darf (s. Verwendung zusätzlicher ViPNet Komponenten auf S. 123). Versuchen Sie das Programm ViPNet Business Mail ohne diese

Erlaubnis zu starten, wird eine entsprechende Meldung auf den Clients angezeigt, dabei können Sie mit dem Programm nicht arbeiten.

Ausführliche Informationen zum Programm „Business Mail" finden Sie im Abschnitt Arbeit mit ViPNet Business Mail (auf S. 228).

ViPNet Programmkontrolle

Das Programm ViPNet Programmkontrolle ermöglicht die Überwachung von Netzwerkaktivitäten der auf dem Computer installierten Anwendungen. Folgende Netzwerkaktivitäten werden von ViPNet Programmkontrolle überwacht:

- Versuche, ausgehende Verbindungen herzustellen.
- Versuche, Ports für eingehende Verbindungen zu öffnen.
- Versenden von Datenpaketen ohne vorhergehenden Aufbau einer Verbindung.

Wählen Sie zum Starten des Programms ViPNet Programmkontrolle im Programm ViPNet Coordinator Monitor im Menü **Anwendungen** den Eintrag **Programmkontrolle**. Nunmehr wird das Programm ViPNet Programmkontrolle beim Start des Betriebssystems automatisch gestartet. ViPNet Programmkontrolle arbeitet unabhängig vom Programm ViPNet Monitor. Wenn ViPNet Monitor aus dem Arbeitsspeicher des Computers entladen wird, setzt das Programm ViPNet Programmkontrolle seine Arbeit fort, bis es vom Benutzer beendet wird.



Hinweis. Das vorliegende Kapitel beinhaltet eine kurze Beschreibung des Programms ViPNet Programmkontrolle. Ausführliche Informationen sind in der Programm-Hilfe enthalten (Aufruf durch Drücken der **F1**-Taste oder über das Menü **Hilfe**).

Integrierte Kommunikationsmittel

Die Software ViPNet Client Monitor und ViPNet Coordinator Monitor beinhaltet eine Reihe nützlicher Anwendungen, die einen schnellen und sicheren Datenaustauschzwischen den Teilnehmern im ViPNet Netzwerk gewährleisten sowie andere Funktionen übernehmen:

- **Chat/Konferenz**. Diese Funktion wird dazu verwendet, kurze Nachrichten zwischen den ViPNet Benutzern in Echtzeit zu übermitteln. Die Anwendung ist vergleichbar mit Programmen wie ICQ, MSN Messenger und AOL Instant Messenger. Der Vorteil der ViPNet Anwendung besteht darin, dass alle Nachrichten verschlüsselt werden.
- **FileExchange**. Diese Funktion ermöglicht den schnellen, unkomplizierten und verschlüsselten Austausch von Dateien zwischen den ViPNet Benutzern, ohne dass zusätzliche Dienste oder Anwendungen (zum Beispiel die Freigabe von Objekten oder FTP-Server) erforderlich sind. Die Funktion ist in Windows Explorer integriert und kann mittels Rechtsklick auf die gewählte Datei oder Ordner über das Kontextmenü aufgerufen werden. Es können Dateien beliebiger Größe versendet werden.

- **Web-Link**. Diese Funktion ermöglicht den Zugang auf die Web-Ressourcen eines geschützten (mit installierter ViPNet Software) Computers. Zwischen den ViPNet Netzwerkknoten werden verschlüsselte Verbindungen aufgebaut.
- **Freigegebene Ordner anzeigen**. Diese Funktion erlaubt es, auf verfügbare freigegebene Netzwerkobjekte eines geschützten (mit installierter ViPNet Software) Computers zuzugreifen. Zwischen den ViPNet Netzwerkknoten werden verschlüsselte Verbindungen aufgebaut.
- **Überprüfung der Verbindung**. Diese Funktion erlaubt es Ihnen, die Verbindung zu einem oder mehreren ViPNet Netzwerkknoten zu überprüfen und Statusinformationen zum gegebenen Netzwerkknoten zu erhalten.

ViPNet Coordinator HW und ViPNet Coordinator VA

Die Funktionen eines Coordinators Ihres ViPNet Netzwerks können von einem spezialisierten Softwaresystem und von einer virtuellen Komponente ausgeführt werden:

- ViPNet Coordinator HW ist ein System, welches sich aus einer bestimmten Hardwareplattform und den darauf installierten Softwaremodulen zusammensetzt. Das System wird in drei verschiedenen Modifikationen (s. Modifikationen von ViPNet Coordinator HW auf S. 34) bereitgestellt.
- ViPNet Coordinator VA ist ein Image der ViPNet Software, welches in einer virtuellen Umgebung installiert und eingesetzt wird. Diese Lösung gibt es in drei verschiedenen Modifikationen (s. Modifikationen von ViPNet Coordinator VA auf S. 34).

Alle Ausführungen von ViPNet Coordinator HW und ViPNet Coordinator VA übernehmen die gleichen Aufgaben im Netzwerk. Im vorliegenden Dokument können sie mit dem allgemeinen Begriff ViPNet Coordinator HW/VA bezeichnet werden. Die grundliegenden Unterschiede zwischen den vorhandenen Modifikationen sind durch die Begrenzungen der Leistungsfähigkeit der Coordinatoren und der Anzahl der unterstützten Netzwerkadapter bedingt.

ViPNet Coordinator HW/VA setzt sich aus einem angepassten Linux Betriebssystem und ViPNet Diensten zusammen, die die grundliegenden Funktionen eines Coordinators implementieren (s. Funktionen des Coordinators im ViPNet Netzwerk auf S. 239):

- Router.
- IP-Adressenserver.
- VPN-Server, der das Routing des geschützten Traffics übernimmt.
- Firewall mit der NAT-Funktion.
- VPN-Gateway, der den Traffic der offenen Knoten tunnelt.
- IPsec-Gateway zum Herstellen von geschützten Verbindungen mit mobilen und Remote-Netzwerken.

ViPNet Coordinator HW/VA verfügt außerdem über zusätzliche Funktionen, die sich zum Aufbau eines lokalen Netzwerks in einem kleineren Büro gut eignen:

- Integrierte DHCP-, DNS- und NTP-Server.
- Proxyserver mit der Möglichkeit, den Inhalt zu filtern und auf Viren zu überprüfen.
- VoIP Server zum Einrichten der internen IP-Telefonie.

Auf virtuellen Geräten ViPNet Coordinator VA und auf Hardware-Modifikationen ViPNet Coordinator HW1000 sowie HW2000 kann auch die Funktion des ViPNet Failover-Systems verwendet werden. Die Technologie ViPNet Failover erlaubt, einen ausfallsicheren Cluster aus zwei Geräten ViPNet Coordinator HW/VA zu erstellen. Ein Gerät davon (aktives) agiert als ViPNet Netzwerkcoordinator, das andere Gerät (passives) befindet sich im Wartemodus. Bei Ausfällen, die für die Funktionsfähigkeit des aktiven Geräts kritisch sind, wechselt das passive Gerät in den Aktivmodus und die Funktion des Coordinators wird aufrechterhalten.

Die Möglichkeit, die Funktion des ViPNet Failover-Systems zu verwenden, wird durch den Netzwerkadministrator im Programm ViPNet Network Manager bei der Verteilung der Lizenzeinschränkungen festgelegt (s. Verwendung zusätzlicher ViPNet Komponenten auf S. 123).

Wenn aus zwei Geräten ViPNet Coordinator HW oder ViPNet Coordinator VA ein Failover-Cluster gebildet werden soll, dann muss zunächst die Verwendung der Software ViPNet Failover auf einem der Coordinatoren im Programm ViPNet Network Manager erlaubt werden. Zusätzlich muss eine Schlüsseldistribution für diesen Coordinator erstellt werden. Im ViPNet Netzwerk stellt der Cluster einen einzelnen Netzwerkknoten dar, deswegen sollte auf beiden Geräten ViPNet Coordinator HW oder ViPNet Coordinator VA die gleiche Schlüsseldistribution installiert werden.



Abbildung 3. Startseite der Webschnittstelle

Ausführliche Informationen zur Software ViPNet Coordinator HW/VA finden Sie im Dokument „ViPNet Coordinator HW/VA. Administratorhandbuch".

Modifikationen von ViPNet Coordinator HW

Die Appliances ViPNet Coordinator HW sind durch drei Modifikationen vertreten. Die Modifikationen verwenden ein Mini-PC als Hardware-Plattform oder ein Server.

Einen Überblick über die vorhandenen Modifikationen von ViPNet Coordinator HW gibt Ihnen die unten angeführte Vergleichstabelle.

Tabelle 3. Modifikationen von ViPNet Coordinator HW

	HW100	HW1000	HW2000
Formfaktorp	Mini-PC	Mini-PC	Server
Ethernet-Adapter	4 x 1 Gbit/s	2-4x 1 Gbit/s	2 x 1 Gbit/d 2 x 10 Gbit/s
Clients registrieren, Gateway-Coordinator-Funktion	ja	ja	ja
ViPNet Failover-Funktion	nein	ja	ja

Für mehrere Informationen, siehe das Dokument „ViPNet Coordinator HW/VA. Administratorhandbuch".

Modifikationen von ViPNet Coordinator VA

Die virtuellen Komponenten ViPNet Coordinator VA sind für die Arbeit in virtuellen Umgebungen VMware Workstation, VMware vSphere und Oracle Virtual Box konzipiert.

Die virtuellen Komponenten ViPNet Coordinator VA gibt es in drei Varianten, die sich anhand der Lizenzbedingungen bezüglich Ihrer Leistungsfähigkeit und der Anzahl der Netzwerkadapter unterscheiden.

Mit Hilfe der unten angeführten Vergleichstabelle können Sie sich einen genaueren Überblick über die Eigenschaften der jeweiligen Modifikation von ViPNet Coordinator VA verschaffen.

Tabelle 4. Modifikationen von ViPNet Coordinator VA

	VA100	VA1000	VA2000
Anzahl der Verkehrsverarbeitungs Kernel-Threads	2	8	16
Ethernet-Adapter	4	4	4

	VA100	VA1000	VA2000
Clients registrieren, Gateway-Coordinator-Funktion	ja	ja	ja
ViPNet Failover-Funktion	ja	ja	ja

Für mehrere Informationen, siehe das Dokument „ViPNet Coordinator HW/VA. Administratorhandbuch".

ViPNet Client for Mac OS X

Die Software ViPNet Client for Mac OS X wird dazu verwendet, den Netzwerktraffic eines mit dem ViPNet Netzwerk oder mit dem Internet verbundenen Computers unter der Steuerung des Betriebssystems Mac OS X zu schützen. Der Schutz des Traffics wird mittels der Funktion der Verschlüsselung und Filterung von IP-Paketen verwirklicht. Mit Hilfe dieser Software können geschützte Verbindungen zu ViPNet Netzwerkknoten oder Knoten, die von ViPNet Coordinatoren getunnelt werden, aufgebaut werden, um einen Zugang zu den Ressourcen dieser Knoten zu erhalten.

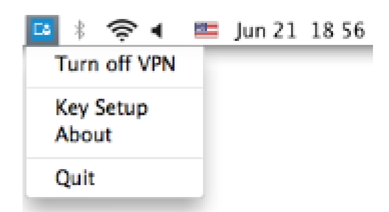


Abbildung 4. Menü der Anwendung ViPNet Client for Mac OS X

ViPNet Client for Android

Die Anwendung ViPNet Client for Android dient dem Schutz des Traffics bei Verbindungen eines Geräts auf Basis des Betriebssystems Android zum geschützten ViPNet Netzwerk oder zum Internet. Der Schutz des Traffics wird durch die Verschlüsselung, Entschlüsselung und Filterung der IP-Pakete sichergestellt. Mit Hilfe dieser Anwendung kann das Gerät eine geschützte Verbindung zu ViPNet Netzwerkknoten bzw. Knoten, die durch ViPNet Coordinatoren getunnelt werden, aufbauen und auf die Ressourcen der gegebenen Knoten zugreifen.

Mit Hilfe der Anwendung ViPNet Client for Android kann der Anwendungstraffic beliebiger Art beim Arbeiten mit Android-Geräten geschützt werden. Unter anderem kann ein geschützter Zugang zum unternehmensinternen Webportal, E-Mail, IP-Telefoniesystem, unterschiedlichen Servern und Internetressourcen sichergestellt werden.

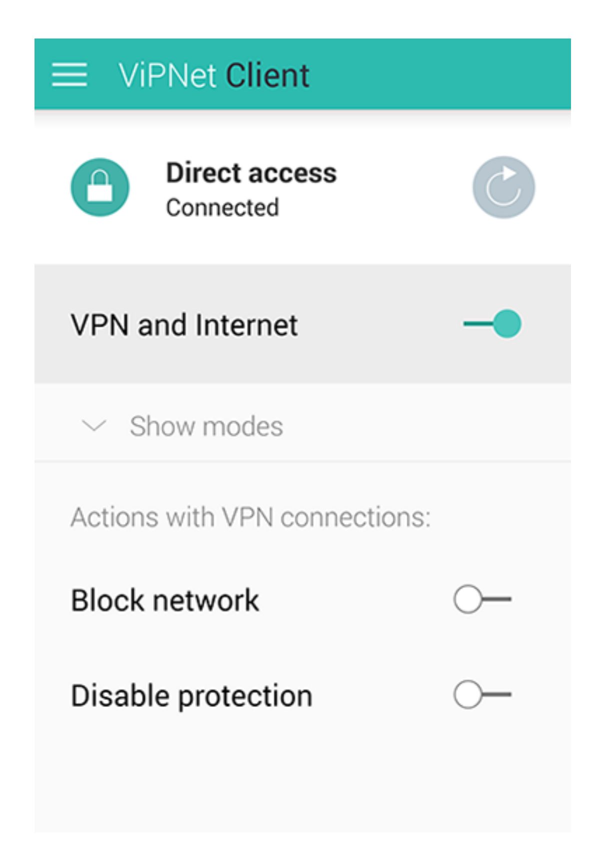


Abbildung 5. ViPNet Client for Android

ViPNet ThinClient

ViPNet ThinClient ist eine integrierte Hard- und Softwarelösung, die eine abgesicherte Benutzer-Arbeitsstation bereitstellt und die Funktionen eines Terminalclients (s. Terminal (Terminalclient) auf S. 373) übernimmt. Mit Hilfe von ViPNet ThinClient kann der geschützte Zugriff auf folgende Elemente sichergestellt werden:

- Remotedesktop auf einem Terminalserver Windows Server 2003/2008 (über das RDP-Protokoll) oder Citrix XenApp (über das ICA-Protokoll).
- Virtueller Desktop VMware Horizon View (über die Protokolle RDP und PCoIP).
- Veröffentlichte Anwendungen auf dem Server Citrix XenApp (über die Protokolle ICA, HTTP).
- Dienste, die auf Basis der Web Access-Technologie implementiert wurden (über die Protokolle HTTP und HTTPS).

ViPNet ThinClient stellt einen Client des ViPNet-Netzwerks dar, der die Verschlüsselung des IP-Traffics durchführt und die Funktionen einer privaten Firewall erfüllt. Dadurch wird der Schutz des Terminalclients vor Netzwerkangriffen und nicht erwünschten Eingriffen in die Terminalsitzung des Benutzers sichergestellt.

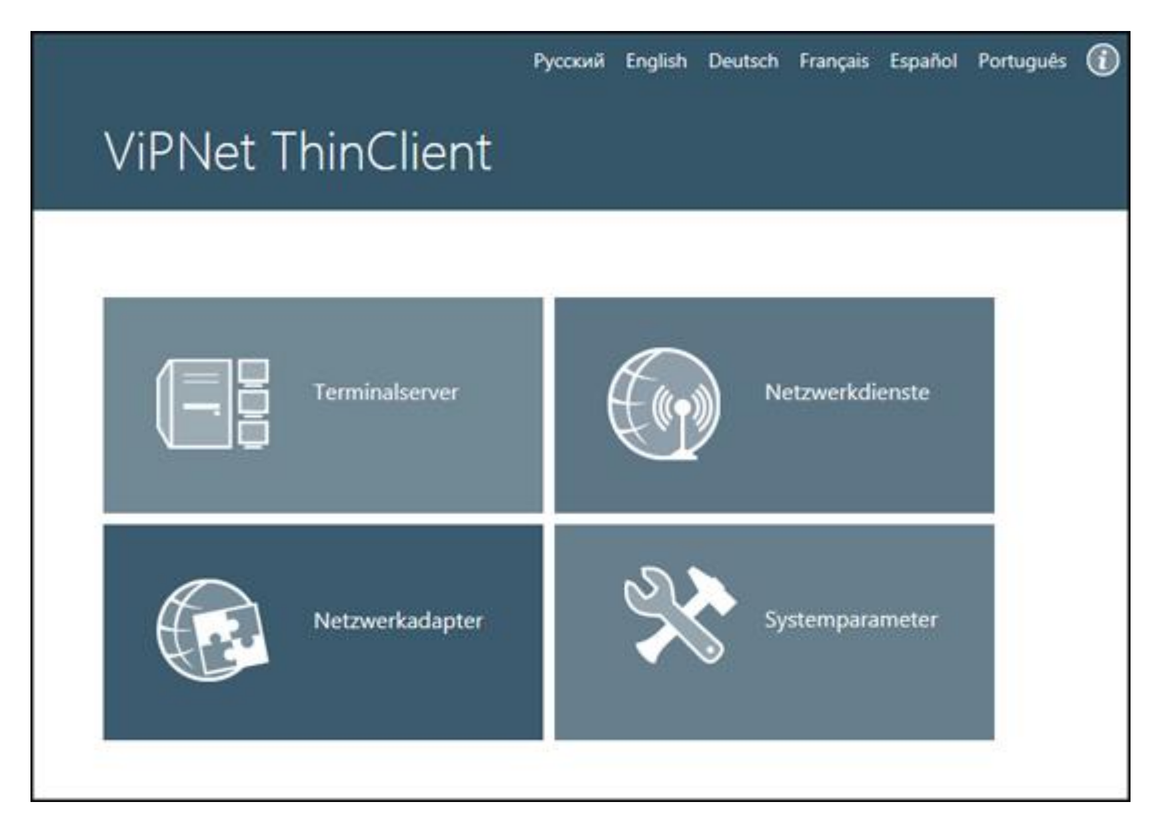


Abbildung 6. Startseite der Einstellungen von ViPNet ThinClient

Ausführliche Informationen zu ViPNet ThinClient finden Sie im Dokument „ViPNet ThinClient. Administratorhandbuch“.

ViPNet Policy Manager

Das Programm ViPNet Policy Manager wird dazu verwendet, die Sicherheitsrichtlinien der Netzwerkknoten, auf denen die Software ViPNet Client oder ViPNet Coordinator installiert ist, zentralisiert zu verwalten. Die Sicherheitsrichtlinien beinhalten Netzwerkfilter (auf S. 371) und NAT-Regeln (s. Netzwerkadressenübersetzung (NAT) auf S. 371). Der Administrator des Programms ViPNet Policy Manager kann zum Beispiel den Internet-Zugang für die Netzwerkknoten während der Nacht sperren oder Verbindungen zu bestimmten Ressourcen blockieren.

In einem ViPNet Netzwerk unter der Steuerung des Programms ViPNet Network Manager kann die Software ViPNet Policy Manager nur auf die Netzwerkclients installiert werden. Eine Installation auf dem Coordinator ist nicht möglich. Für die Verwendung der Software ViPNet Policy Manager im Netzwerk wird eine entsprechende Lizenz benötigt (s. Verwendung der Software ViPNet Policy Manager auf S. 120).

Die Liste der von ViPNet Policy Manager gesteuerten Knoten wird auf der Registerkarte **Verwaltete Netzwerkknoten** des entsprechenden Clients festgelegt. Eine Aktualisierung der Liste der verwalteten Knoten im Programm ViPNet Policy Manager erfolgt beim Versand von Schlüsselupdates.

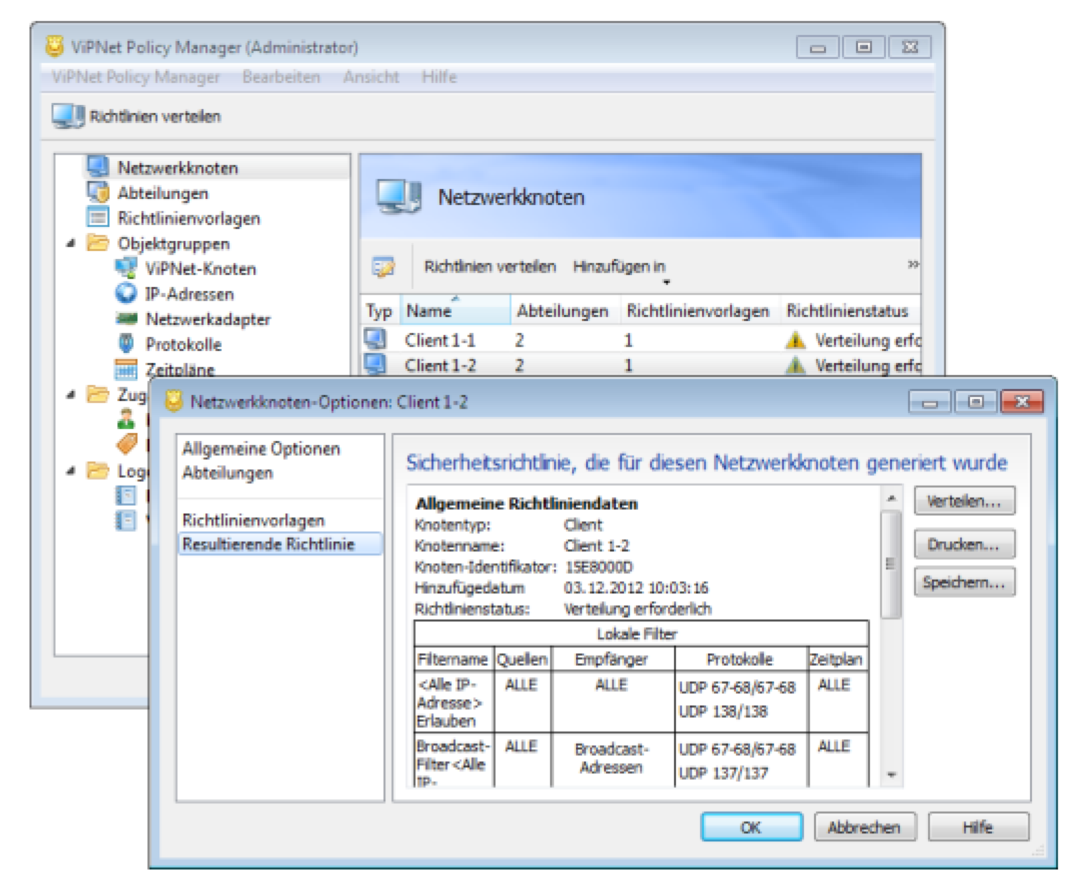


Abbildung 7. Programm ViPNet Policy Manager

Ausführliche Informationen zur Verwendung des Programms ViPNet Policy Manager finden Sie im Dokument „ViPNet Policy Manager. Administratorhandbuch“.

ViPNet StateWatcher

Das Softwaresystem zur Überwachung von geschützten Netzwerken ViPNet StateWatcher dient der Statusüberwachung von ViPNet Netzwerkknoten, der Kontrolle von Sicherheitsereignissen auf den Knoten, der frühzeitigen Identifizierung von Störfällen im Betrieb der Knoten und der rechtzeitigen Benachrichtigung der Benutzer über auftretende Probleme. Die Softwarelösung ViPNet StateWatcher ermöglicht es dem Benutzer, Informationen über den Status von Knoten, auf denen keine ViPNet Software installiert ist, über das SNMP-Protokoll zu erhalten.

Eine Basiskomponente der Softwarelösung ViPNet StateWatcher stellt die Software Monitoring-Server dar, die Daten über den aktuellen Status der ViPNet Netzwerkknoten (Monitoring-Hosts) und der darauf installierten Software erhebt. Auf Basis der erhaltenen Informationen stellt Monitoring-Server fest, ob die Knoten ordnungsgemäß funktionieren, und benachrichtigt im Fall von Störungen oder kritischen Ereignissen die Benutzer (zum Beispiel mittels E-Mail oder SMS).

Zur Steuerung des Monitoring-Servers wird die gesonderte Web-Schnittstelle verwendet (sog. „Arbeitsplatz für Monitoring“ auf dem Bild unten). Der Monitoring-Server kann nur von einem geschützten Netzwerkknoten mit installierter ViPNet Client-Software gesteuert werden.

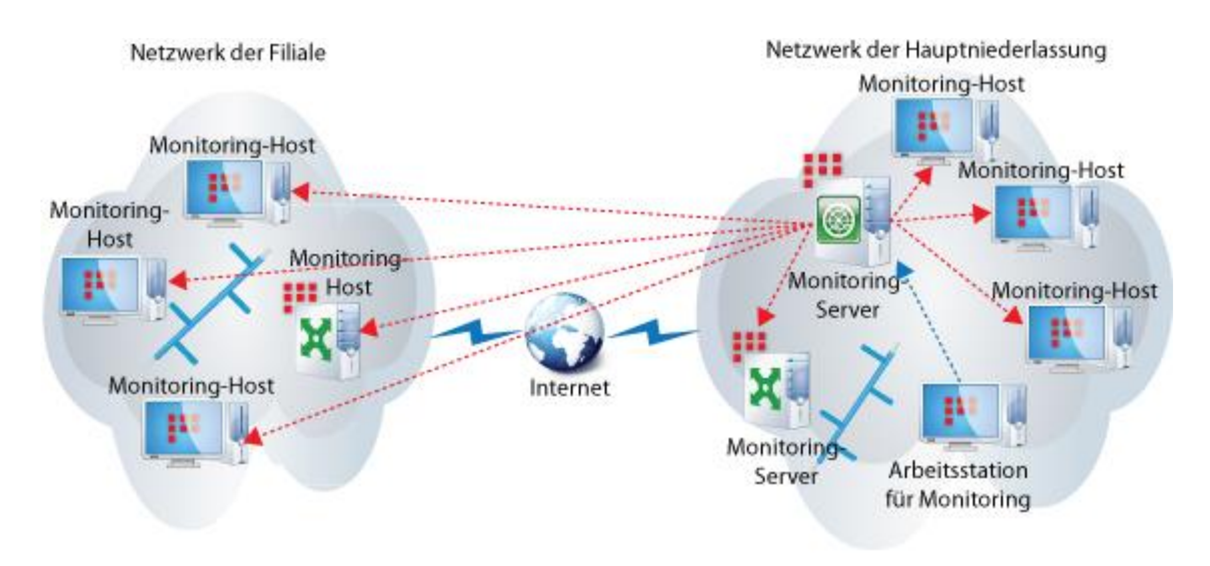


Abbildung 8. Aufbauschema eines Überwachungssystems für verteilte ViPNet-Netzwerke

Innerhalb des ViPNet Netzwerks, das sich unter der Verwaltung des Programms ViPNet Network Manager befindet, kann die Software Monitoring-Server ausschließlich auf Clients installiert werden. Eine Installation auf dem Coordinator ist nicht möglich. Für die Verwendung der Softwarelösung ViPNet StateWatcher im Netzwerk wird eine entsprechende Lizenz (s. Verwendung der Software ViPNet StateWatcher auf S. 120) benötigt.

In der Software Monitoring-Server werden alle Netzwerkknoten automatisch zur Liste der Monitoring-Hosts hinzugefügt. Eine Aktualisierung der Liste der Monitoring-Hosts (zum Beispiel beim Hinzufügen neuer Hosts) wird beim Versand von Schlüsselupdates durchgeführt.

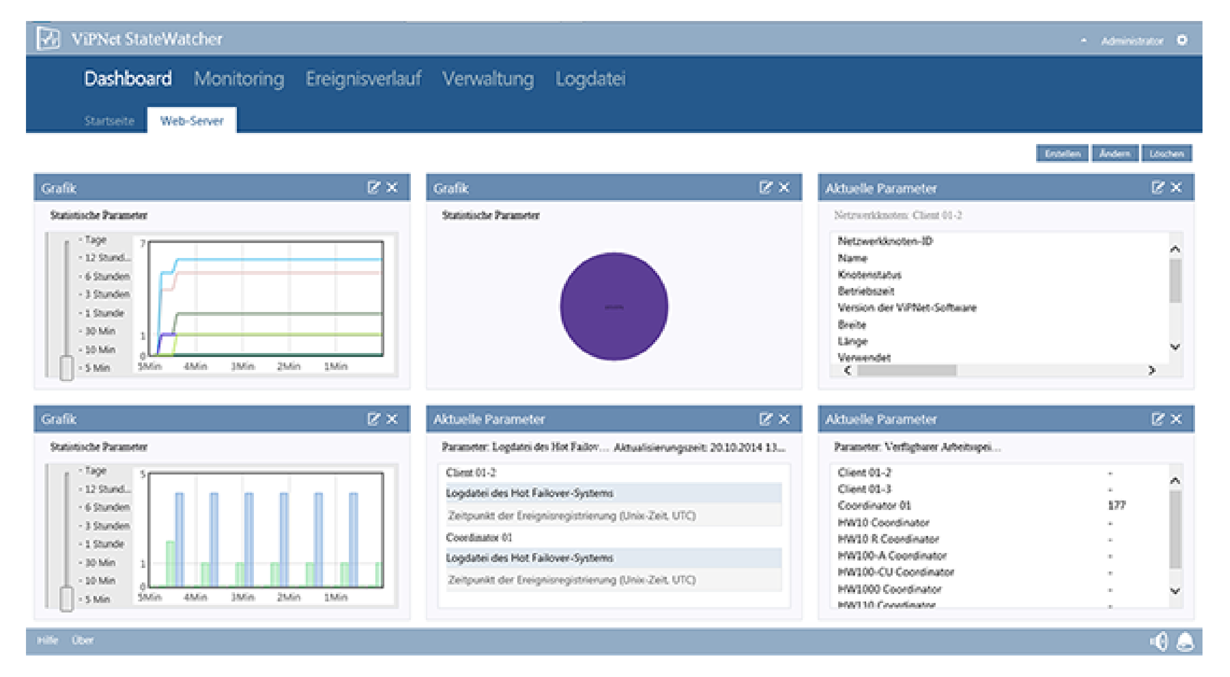


Abbildung 9. Programm ViPNet StateWatcher

Ausführliche Informationen zur Verwendung des Überwachungssystems finden Sie in der Dokumentation von ViPNet StateWatcher.

ViPNet SafeDisk-V

Das Programm ViPNet SafeDisk-V ist dazu bestimmt, vertrauliche Daten, die auf der Festplatte oder auf einem mobilen Datenträger gespeichert sind, zu schützen.

Die zu schützenden Daten werden in einem SafeDisk-V-Container abgelegt. Der Container stellt eine verschlüsselte Datei dar. Nach dem Einbinden des Containers im Programm ViPNet SafeDisk-V wird dieser im Betriebssystem wie ein logisches Laufwerk abgebildet.

Beim Speichern von Daten im eingebundenen Container werden diese automatisch verschlüsselt. Beim Auslesen der Daten werden diese automatisch entschlüsselt. Die Verschlüsselung erfolgt im Hintergrund, ist für den Benutzer nicht erkennbar und erfordert keine zusätzlichen Eingriffe.

Nach dem Trennen wird der Container nicht mehr im System abgebildet. Die Präsenz von vertraulichen Informationen ist nicht mehr erkennbar, der Zugriff auf die Daten ist nicht mehr möglich.

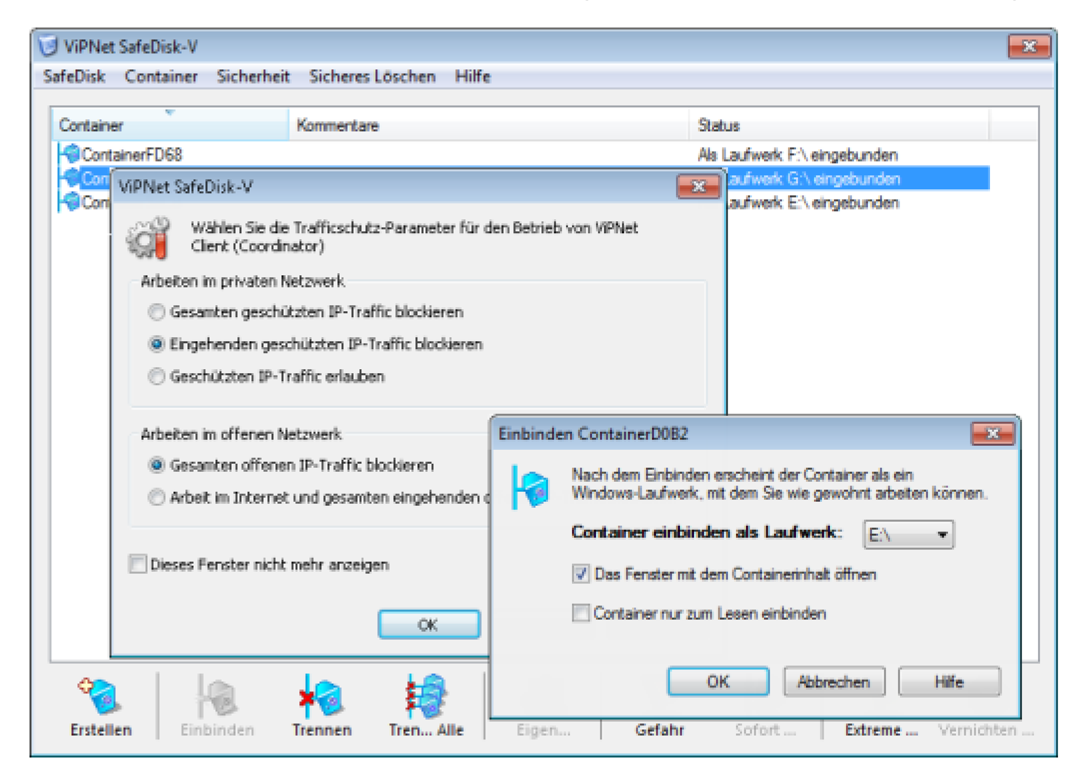


Abbildung 10. Programm ViPNet SafeDisk-V

Das Programm ViPNet SafeDisk-V kann lediglich zusammen mit dem Programm ViPNet Client auf dem Computer funktionieren, wenn der Netzwerkadministrator es erlaubte, ViPNet SafeDisk-V auf dem Netzwerkknoten im Programm ViPNet Network Manager zu verwenden (s. Verwendung zusätzlicher ViPNet Komponenten auf S. 123). Die Zahl der Netzwerkknoten, auf denen ViPNet SafeDisk-V funktionieren kann, ist durch die Lizenz ViPNet VPN (s. Lizenzierung von ViPNet VPN auf S. 47) eingeschränkt.

Das Programm ViPNet SafeDisk-V, das mit ViPNet Client zusammen funktioniert, bietet die folgenden Vorteile:

- Nur der Netzwerkknotenbenutzer besitzt Zugang zu den Containern;

- Schlüssel müssen nicht selbständig aktualisiert werden.

  Beim gemeinsamen Einsatz von ViPNet SafeDisk-V und ViPNet Client wird das Update der Containerschlüssel von ViPNet SafeDisk-V zusammen mit dem Update der Netzwerkknoten- und ViPNet Benutzerschlüssel durchgeführt. Dies ist möglich, da die Containerschlüssel durch Netzwerkknoten- und ViPNet Benutzerschlüssel geschützt sind.

ViPNet Connect

Das Programm ViPNet Connect ist für Sprachanrufe der Benutzer des ViPNet Netzwerkes über einen geschützten VPN-Kanal gedacht. Die Kontaktliste jedes Benutzers setzt sich im Programm ViPNet Network Manager zusammen. Die Knoten sollen dazu im ViPNet Netzwerk verbunden sein, und es soll erlaubt sein, mit dem Programm ViPNet Connect zu arbeiten (s. Verwendung zusätzlicher ViPNet Komponenten auf S. 123).

Das Programm ViPNet Connect kann auf die Clients mit der ausgebauten Software ViPNet Client für Windows, ViPNet Client for Android oder ViPNet Client for Mac OS X installiert werden.

Grundlegende Funktionen von ViPNet VPN

ViPNet Network Manager

Das Programm ViPNet Network Manager ermöglicht es Ihnen, folgende Aufgaben zu erfüllen:

- Aufbau der ViPNet Netzwerktopologie;
- Zentralisierte Konfiguration der Netzwerkknoten;
- Erstellung der Netzwerkknotenschlüssel;
- Zentralisierte Aktualisierung der Netzwerkknotenschlüssel;
- Zentralisierte Konfiguration der Firewalleinstellungen und der Tunnelung des VPN-Traffics;
- Zentralisierte Definition der DNS-Namen;
- Anbindung von Clients mit Betriebssystem Android oder iOS mit Hilfe der IPsec-Technologie;
- Unterstützung von Clients, auf denen die Software ViPNet Client (Windows) oder ViPNet Client for Mac OS X und ViPNet Client for Android installiert ist, sowie von Clients vom Typ ViPNet ThinClient.
- Zentralisierte Verwaltung der Parameter von IPsec-Verbindungen zu anderen Netzwerken über einen Coordinator, auf dem die Software ViPNet Coordinator HW/VA installiert ist;
- Zentralisierte Verwaltung der IPsec-Verbindungsparameter mobiler Clients mit Betriebssystem iOS;
- Einrichtung von Partnernetzwerk-Verbindungen mit anderen VPN-Netzwerken;
- Verwaltung der Netzwerkknoten-Sicherheitsrichtlinien mit Hilfe des Programms ViPNet Policy Manager;
- Zentralisierte Überwachung der Netzwerkknoten-Status mit Hilfe der Software ViPNet StateWatcher;
- Erstellung von Sicherungskopien (Backup) der Programmkonfigurationen;
- Flexible Lizensierung.

ViPNet Client für Windows

Das Programm ViPNet Client ermöglicht es Ihnen, folgende grundlegende Aufgaben zu lösen:

- Verschlüsselung des ein- und ausgehenden IP-Traffics;
- Unterstützung der Verschlüsselungsalgorithmus AES;
- Trennung der Arbeit mit geschütztem und mit öffentlichem Traffic;
- Filterung des Traffics nach IP-Adressen und Ports des Ziel- und Quellknotens;

- Transparentes Arbeiten mit geschütztem Traffic ohne Verwendung der Technologie der Serververbindung;
- Bezug statistischer Daten über den blockierten Traffic;
- Analyse der ein- und ausgehenden IP-Pakete mit der Möglichkeit, diese Daten in eine Datei zu exportieren;
- Möglichkeit der gleichzeitigen Arbeit nach dem Schema „point-to-multipoint";
- Bezug aktueller Informationen über den Status von ViPNet Netzwerkknoten und insbesondere über die Zugangs-IP-Adressen dieser Knoten;
- Verschlüsselter Austausch von Dateien und Nachrichten mit anderen ViPNet Netzwerkknoten;
- Erhalt von zentralisierten Updates der Schlüssel und der Software ViPNet Client;
- Überwachung des Zustands von Knoten mit installierter ViPNet Client-Software mit Hilfe des zentralisierten Monitoringsystems ViPNet StateWatcher;
- Unterstützung von 32- und 64-Bit-Betriebssystemen.

ViPNet Coordinator für Windows

Das Programm ViPNet Coordinator ermöglicht es Ihnen, folgende grundlegende Aufgaben zu lösen:

- Verschlüsselung des ein- und ausgehenden IP-Traffics;
- Unterstützung der Verschlüsselungsalgorithmus AES;
- Trennung der Arbeit mit geschütztem und mit öffentlichem Traffic;
- Filterung des Traffics nach IP-Adressen und Ports des Ziel- und Quellknotens;
- Ziel- und Quelladressübersetzung;
- Bezug statistischer Daten über den blockierten Traffic;
- Analyse der ein- und ausgehenden IP-Pakete mit der Möglichkeit, diese Daten in eine Datei zu exportieren;
- Einsatz als Kommunikationsserver für die Übermittlung von Schlüssel- und Softwareupdates, Dateien und Nachrichten zwischen den Benutzern;
- Einrichtung des Zugangs lokaler Netzwerkknoten zum Internet und des Zugangs zu diesen Knoten aus dem Internet unter Verwendung der Quell- und Ziel-IP-Adressenübersetzung;
- Aufbau von geschützten Verbindungen zu Knoten, auf denen keine ViPNet Software installiert ist, mit Hilfe der Technologie der Tunnelung;
- Verhinderung der Überschneidung und Substitution von IP-Adressen mit Hilfe der Technologie der virtuellen IP-Adressen;
- Bezug aktueller Informationen über den Status von ViPNet Netzwerkknoten und insbesondere über die Zugangs-IP-Adressen dieser Knoten;

- Überwachung des Zustands von Knoten mit installierter ViPNet Coordinator-Software mit Hilfe des zentralisierten Monitoringsystems ViPNet StateWatcher;
- Unterstützung von 32- und 64-Bit-Betriebssystemen.

Beschaffung erforderlicher Informationen

In den meisten Fällen entspricht die logische ViPNet Struktur (Verteilung der Clients und deren Anbindung an die Coordinatoren) der existierenden physikalischen Netzwerkstruktur. Entsprechend der eingesetzten Sicherheitsrichtlinie kann der Coordinator eine oder mehrere Funktionen erfüllen (s. Funktionen des Coordinators im ViPNet Netzwerk auf S. 239).

Sowohl der Coordinator als auch der Client können dazu verwendet werden, den Traffic bestimmter (oder aller) Dienste und Anwendungen auf dem Server (zum Beispiel Domänenkontroller, SMTP-/FTP-/Webserver, Datenbankserver u. s. w.) zu schützen.

Damit eine optimale Konfiguration des ViPNet Netzwerks bestimmt werden kann, sollten die folgenden Fragen beantwortet werden:

- Welche logische Struktur des VPN-Netzwerks passt am besten zur bestehenden physikalischen Netzwerkstruktur?
- Wie viele Arbeitsstationen, Server und Segmente des lokalen Netzwerks sollten geschützt werden?
- Auf welchen Netzwerkknoten (Client oder Coordinator) die Arbeitsstation des ViPNet Administrators installiert werden muss?
- Soll das Monitoringsystem für die Netzwerkknoten ViPNet StateWatcher (auf S. 38) verwendet werden?
- Sollen Coordinatoren auf separaten Computern installiert werden oder können sie mit vorhandenen Servern/Arbeitstationen kombiniert werden?
- Wie sollen integrierte Firewalls konfiguriert werden, um einen ordnungsgemäßen Betrieb des Netzwerks und der Netzwerkdienste zu gewährleisten? Zum Beispiel werden Clients und Coordinatoren den eingehenden unverschlüsselten Traffic standardmäßig blockieren.
- Sollen die Sicherheitsrichtlinien (Firewallparameter) der Netzwerkknoten mit Hilfe des Programms ViPNet Policy Manager (auf S. 37) zentralisiert verwaltet werden?

Zusätzlich sollten vom Administrator des ViPNet Netzwerks folgende Daten erhoben werden:

- Benötigte Anzahl an ViPNet Knoten;
- Für jedes Segment des lokalen Netzwerks:
  - Anzahl der Server, die in das ViPNet Netzwerk eingebunden werden sollen;
  - Betriebssystemen für diese Server;
  - Andere eingesetzte Sicherheitssoftware (Firewalls, Antivirus-Programme, andere Software);
  - Typ des Traffics zwischen Segmenten/Servern/Arbeitstationen (verwendete Dienste, Protokolle, Portnummern);
  - Verwendete IP-Adressen der Server (öffentliche oder private);

- Wie findet der Zugriff auf die Server und Gateways von außen statt? Wie sind das Routing des ein- und ausgehenden Datenverkehrs und die Netzwerkadressenübersetzung (NAT) organisiert? Welche Arten von Firewalls sind im Einsatz, wird Netzwerkadressenübersetzung (NAT) verwendet? Ein detailliertes Schema der Netzwerktopologie sollte aufgezeichnet werden.
- Welche Anwendungen sollen mit Hilfe von VPN geschützt werden (Datenbanken, CRM/CMS/ERP-Systeme, Web-Anwendungen u. s. w.)?

- Struktur der verschlüsselten Verbindungen (wer mit wem?):
  - zwischen den unterschiedlichen lokalen Segmenten;
  - zwischen den einzelnen VPN-Clients.

Lizenzierung von ViPNet VPN

Lizenzarten im ViPNet VPN

Gegenwärtig wird ViPNet VPN in Form folgender Pakete geliefert: Demo (nicht registrierte Version) und Light (registrierte Version). Jedes Paket beinhaltet eine Lizenz, welche die maximale Anzahl an Coordinatoren und Clients unterschiedlicher Typen festlegt.

Sie können auch eine Lizenz für eine beliebige Anzahl von Coordinatoren und Clients erwerben. Dazu wenden Sie sich bitte an Infotecs GmbH.



Hinweis. Sie können auch eine bereits vorhandenen Lizenz erweitern und dadurch die Anzahl der Coordinatoren, Clients und Smartphone-Clients erhöhen. Mehr Informationen finden Sie weiter unten (s. Lizenzerweiterung auf S. 48).

Einschränkungen der kostenlosen Version

Ab dem Zeitpunkt des ersten Starts arbeitet das Programm ViPNet Network Manager wie eine nicht registrierte Version und unterliegt den folgenden Einschränkungen:

- Das Programm kann nur während der nächsten 60 Tage verwendet werden, danach kann dieses nicht mehr gestartet werden.
- Folgende Elemente können erstellt werden:
  - Zwei Coordinatoren vom Typ ViPNet Coordinator Windows.
  - Einen Coordinator vom Typ ViPNet Coordinator VA100.
  - Einen Coordinator vom Typ ViPNet Coordinator VA1000.
  - Zehn Clients vom Typ ViPNet Client Windows oder ViPNet Client for Mac OS X.
  - Zehn Clients vom Typ ViPNet ThinClient.
  - Zehn Clients vom Typ ViPNet Client for Android.
  - Fünf Clients vom Typ ViPNet Client iOS IPsec.
- Das Programm ViPNet Policy Manager kann auf einem Knoten verwendet werden. Es können damit 10 Knoten gesteuert werden.
- Die Lösung ViPNet StateWatcher kann verwendet werden, es können bis zu zehn Monitoring-Hosts überwacht werden.
- Die Funktion des ViPNet Failover-Systems kann auf Netzwerkknoten ViPNet Coordinator VA100 und ViPNet Coordinator VA1000 verwendet werden.

- Die Programme ViPNet Business Mail, ViPNet Connect und ViPNet SafeDisk-V können auf bis zu zehn Clients verwendet werden.
- Zwei Coordinatoren können als IPsec-Gateways verwendet werden.
- Schlüssel für Netzwerkknoten gelten nur 60 Tage lang. Nach dem Ablauf von 60 Tagen funktioniert die auf Netzwerkknoten installierte ViPNet Software nicht mehr. Bitte beachten Sie dieses bei der Installation der kostenlosen Version in einem Netzwerk, das in realen Geschäftsprozessen verwendet wird.
- Sie können keine Partnernetzwerkverbindung aufbauen.

Um den ViPNet Network Manager nach Ablauf der Gültigkeitsdauer der Demo-Version verwenden zu können und damit es möglich wird, die den Bedürfnissen des Unternehmens entsprechende Netzwerkstruktur aufzubauen, müssen Sie das Programm registrtieren (s. Registrierung von ViPNet Network Manager auf S. 70).

Wenn gemäß Ihrer ViPNet VPN-Lizenz nach dem Registrieren des Programms ViPNet Network Manager eine geringere Anzahl an Netzwerkknoten erstellt werden kann, als die Anzahl der Knoten, die vor der Programmregistrierung mit Hilfe der Demolizenz angelegt wurden, dann sollten Sie Folgendes beachten:

- Im Hauptfenster des Programms ViPNet Network Manager wird in der Navigationsleiste beim Auswählen des Elements **Eigenes Netzwerk** in der Panel-Ansicht neben dem Inhalt der Lizenz auch eine Meldung über die Überschreitung der zulässigen Grenze angezeigt.
- Im Programm ViPNet Network Manager können keine neuen Knoten angelegt und keine Schlüsseldistributionen mehr erstellt und versendet werden.

Entfernen Sie in diesem Fall die überflüssigen Netzwerkknoten aus dem Programm ViPNet Network Manager oder wenden Sie sich an einen Vertreter der Firma Infotecs, um eine Lizenzerweiterung zu beantragen (s. Lizenzerweiterung auf S. 48).

Lizenzerweiterung

Wenn Sie die maximale Anzahl an Netzwerkknoten oder die Anzahl an Lizenzen für die unterschiedlichen Typen von Coordinatoren und Clients sowie für zusätzliche Programme erhöhen möchten, dann wenden Sie sich an einen Vertreter der Infotecs GmbH und bestellen Sie eine neue Lizenz für das ViPNet Netzwerk.

Dafür benötigt der Infotecs-Vertreter die Nummer des bereits eingerichteten Netzwerks sowie die gewünschten Eckdaten der neuen Lizenz. Um die Nummer des Netzwerks zu ermitteln, wählen Sie im Programm ViPNet Network Manager in Menü **Hilfe** die Option **Über ViPNet Network Manager** aus.

Nach der Bearbeitung Ihrer Anfrage zur Lizenzerweiterung erhalten Sie eine neue Lizenzdatei mit der Erweiterung `.reg` oder `.itcslic`. Importieren Sie die Lizenz (s. Import der neuen Lizenz auf S. 49) im Programm ViPNet Network Manager.

Auf gleiche Weise können die Appliance oder virtuelles Gerät ViPNet Coordinator HW/VA erworben und eingerichtet werden. Um mehr über die Software- und -Hardware-Lösungen von ViPNet zu erfahren,

welche gemeinsam mit der Software ViPNet VPN eingesetzt werden können, wenden Sie sich an Infotecs GmbH.

Import der neuen Lizenz

Nachdem Sie die aktualisierte Lizenzdatei mit dem Erweiterung `.reg` oder `.itcslic` (s. Lizenzerweiterung auf S. 48) erhalten haben, sollten Sie diese im Programm ViPNet Network Manager importieren. Neue Lizenzeinschränkungen treten dabei automatisch in Kraft, ein Neustart des Programms ist dazu nicht erforderlich.

Führen Sie die folgenden Schritte durch, um die Lizenzdatei zu importieren:

1 Klicken Sie im Hauptprogrammfenster von ViPNet Network Manager im Menü **Hilfe** auf den Befehl **Lizenzdatei laden**.

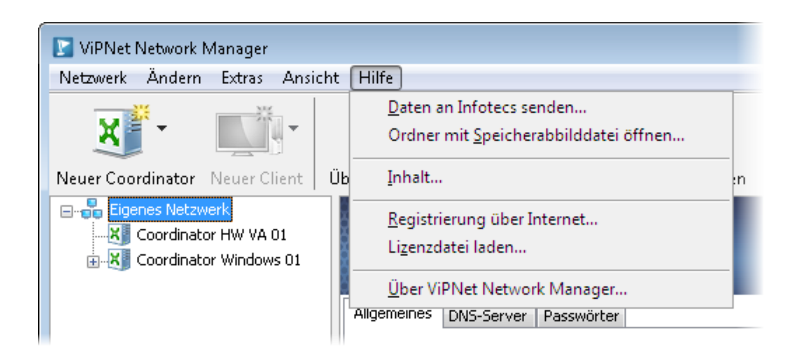


Abbildung 11. Import der Lizenzdatei

2 Wählen Sie im eingeblendeten Fenster die benötigte Lizenzdatei aus und klicken Sie auf **Öffnen**.

Ihre ViPNet VPN-Lizenz wird nun aktualisiert.

2

Installation und Deinstallation von ViPNet VPN

Vorgehensweise beim Installation von ViPNet VPN

ViPNet VPN stellt eine Zusammensetzung von Komponenten dar, mit deren Hilfe sich virtuelle private Netzwerke (s. Virtuelles Privates Netzwerk (VPN) auf S. 374) basierend auf ViPNet Technologie aufbauen lassen.

Die Software ViPNet VPN kann mit Hilfe der Installationsdatei der Demoversion von ViPNet VPN installiert werden, die auf der Webseite http://infotecs.de/download/ zum Download bereitgestellt ist.

Führen Sie alle Tasks aus der nachfolgenden Liste aus, um die primäre Installation der Software ViPNet VPN durchzuführen und ein neues ViPNet Netzwerk zu erstellen.

Wenn ViPNet VPN auf die Version 4.x aktualisiert werden soll, folgen Sie den Anweisungen im Abschnitt Upgrade von ViPNet VPN Version 3.x auf Version 4.x (auf S. 62).



Hinweis. Einige Schritte beziehen sich auf untergeordnete Tabellen mit Aufgaben, welche jeweils komplett abgearbeitet werden sollen, bevor man zum nächsten Schritt der aktuellen Tabelle übergeht.

Wenn der Link zu einem Kapitel mit allgemeinen Informationen führt, machen Sie sich mit diesen Informationen vertraut und gehen Sie danach zum nächsten Schritt über.

	Aufgabe	Link
☐	Planen Sie die Installation von ViPNet VPN genau durch. Sammeln Sie zunächst alle Informationen zur physikalischen und logischen Struktur Ihres Netzwerks.	Beschaffung erforderlicher Informationen (auf S. 45)
☐	Erstellen Sie den Manager-Arbeitsplatz. Installieren Sie das Programm ViPNet Network Manager.	Installation von ViPNet Network Manager (auf S. 53)
☐	Registrieren Sie das Programm ViPNet Network Manager.	Registrierung von ViPNet Network Manager (auf S. 70)
☐	Erstellen Sie das ViPNet Netzwerk und speichern die Schlüsseldistributionen für Netzwerkknoten.	Erstellen des ViPNet Netzwerks (auf S. 86)
☐	Installieren Sie auf der Arbeitsstation des ViPNet Administrators die ViPNet Client- oder ViPNet Coordinator-Software.	Installation von ViPNet Client oder ViPNet Coordinator auf dem Manager-Arbeitsplatz (auf S. 55)
☐	Wenn erforderlich, installieren Sie auf dem Manager-Arbeitsplatz die Programme ViPNet Policy Manager und ViPNet StateWatcher.	ViPNet Policy Manager (auf S. 37) ViPNet StateWatcher (auf S. 38)

	Aufgabe	Link
☐	Installieren Sie ViPNet Coordinator-Software auf alle Netzwerkknoten, die als Server im ViPNet Netzwerk eingesetzt werden sollen.	Installation von ViPNet Coordinator auf ViPNet Netzwerkserver (auf S. 57) ViPNet Coordinator HW und ViPNet Coordinator VA (auf S. 32)
☐	Installieren Sie ViPNet Client-Software auf den Arbeitsstationen der Benutzer, die das ViPNet Netzwerk in ihrer täglichen Arbeit verwenden sollen.	Einrichtung der Benutzerarbeitsplätze im ViPNet Netzwerk (auf S. 59) ViPNet Client for Mac OS X (auf S. 35)
☐	Konfigurieren Sie die Parameter und Einstellungen des ViPNet Netzwerks.	Vorgehensweise beim Konfiguration des ViPNet Netzwerks (auf S. 107)



Tipp. Wir empfehlen, die Liste auszudrucken, und die einzelnen Schritte nach ihrer Durchführung zu markieren.

Einrichtung des Manager-Arbeitsplatzes

Auf dem Computer, der als Arbeitsstation des ViPNet Netzwerkadministrators eingesetzt wird, sollten die Programme ViPNet Network Manager und ViPNet Client oder ViPNet Coordinator nacheinander installiert werden.

Das Programm ViPNet Network Manager wird dazu verwendet, die logische Struktur Ihres ViPNet Netzwerks zu definieren (Einrichtung der Server, der Benutzer-Arbeitstationen und der Verbindungen dazwischen), sowie die Schlüsseldistributionen und Passwörter für die ViPNet Netzwerkknoten anzulegen. Zum Speichern der ViPNet Netzwerkparameter und ViPNet Network Manager-Einstellungen wird der Datenbank-Server Microsoft SQL Server 2008 R2 Express Edition verwendet. Die Installation der Software Microsoft SQL Server 2008 R2 Express Edition wird automatisch mit Hilfe des Installationsprogramms von ViPNet Network Manager durchgeführt.

Damit der Administrator des ViPNet Netzwerks Verbindungen zu anderen ViPNet Netzwerkknoten aufbauen und Schlüsseldistributionen versenden kann,, sollte auf der Arbeitsstation des Administrators die Software ViPNet Client oder ViPNet Coordinator installiert werden. Der Netzwerkknoten, der als Arbeitsstation des Administrators auftritt, besitzt den Status „Manager-Arbeitsplatz" und wird im Hauptfenster von ViPNet Network Manager durch das Symbol oder gekennzeichnet.

Es wird empfohlen, dass Sie das Programm ViPNet Network Manager auf einem Coordinator (Knoten mit ViPNet Coordinator) installieren, falls es sich um ein kleines ViPNet Netzwerk handelt und das Reservieren eines eigenen Clients für die Arbeitsstation des Administrators nicht zweckmäßig erscheint. In allen anderen Fällen sollte ViPNet Network Manager auf einem Client (Knoten mit ViPNet Client) installiert werden.

Die Arbeitsstation des ViPNet Netzwerkadministrators kann auf folgende Netzwerkknoten installiert werden:

- auf beliebige Clients mit dem Betriebssystem Windows;
- auf Coordinatoren mit dem Betriebssystem Windows.

Installation von ViPNet Network Manager

Zum Installieren von ViPNet Network Manager:

1. Schließen Sie alle Anwendungen.
2. Starten Sie das Installationsprogramm von ViPNet VPN. Der Installationsassistent **Installation von ViPNet VPN** wird ausgeführt.

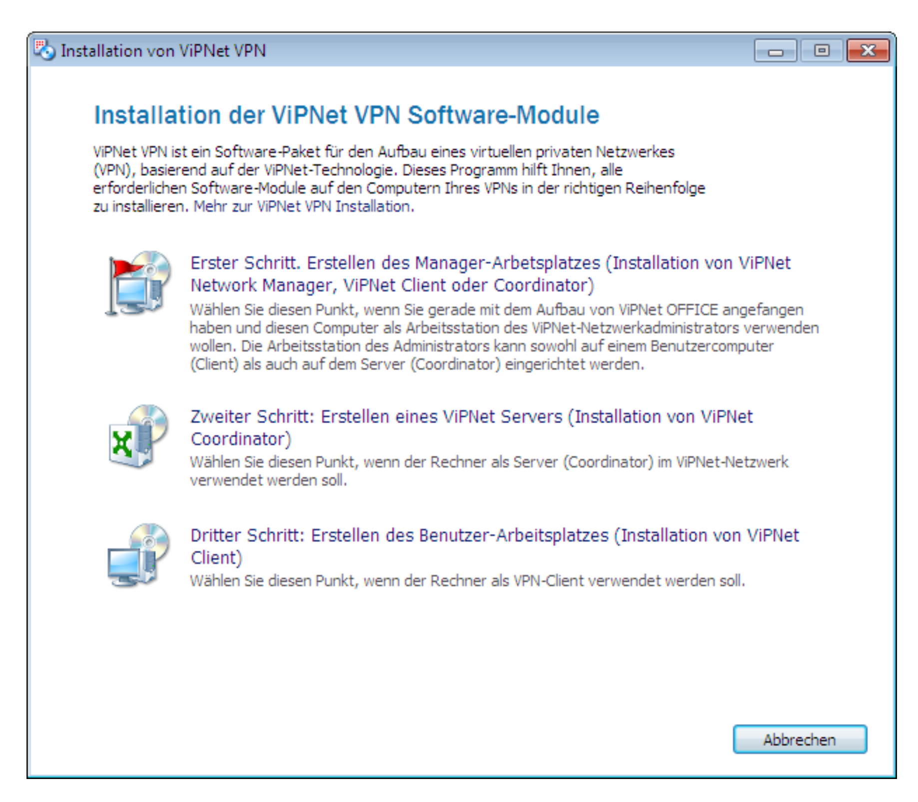


Abbildung 12. Komponenten für die Installation auswählen

3 Klicken Sie im Fenster **Installation der ViPNet VPN Software-Module** auf den ersten Link **Erstellen des Manager-Arbeitsplatzes...**

4 Klicken Sie auf der Seite **Erstellen des Manager-Arbeitsplatzes...** auf die Schaltfläche **ViPNet Network Manager installieren**.

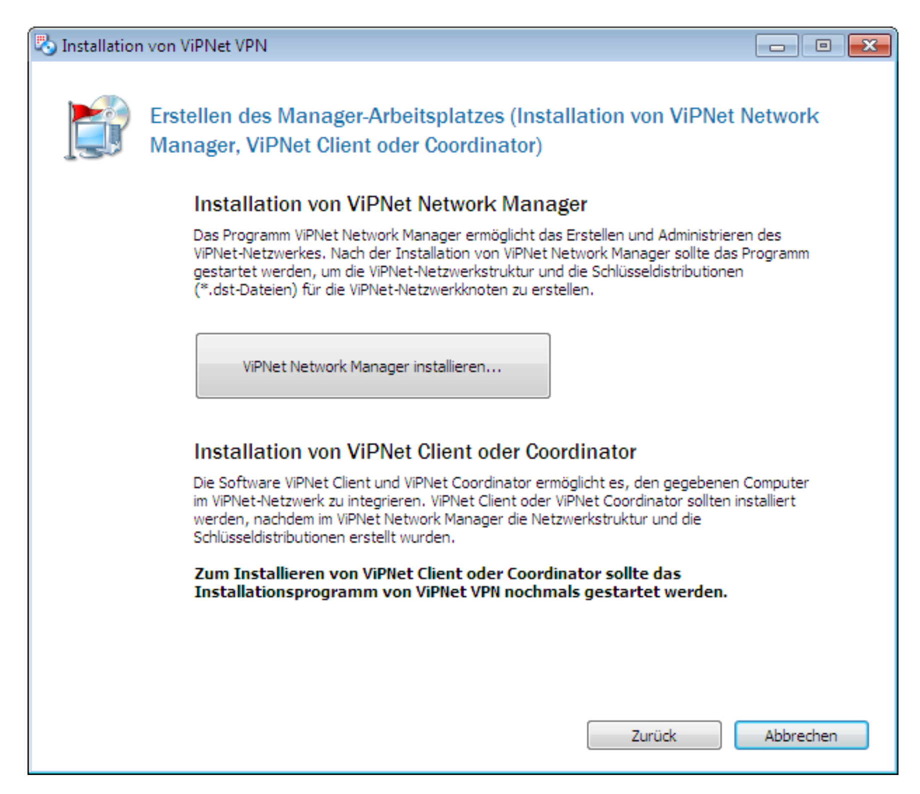


Abbildung 13. Manager-Arbeitsplatz einrichten

5 Wenn Microsoft Windows Installer 4.5 und Microsoft .NET Framework 3.5, das für die Arbeit von ViPNet Network Manager erforderlich ist, nicht auf dem Computer installiert ist, wird eine Meldung mit dem Vorschlag angezeigt, die Software manuell zu installieren. Klicken Sie im Meldungsfenster auf **OK**. Dabei wird die Arbeit des Assistenten **Installation von ViPNet Network Manager** beendet.

   Starten Sie den Assistenten **Installation von ViPNet Network Manager** nach Abschluss der Installation von Microsoft Windows Installer 4.5 und Microsoft .NET Framework 3.5 erneut (wie in Punkt 2–4 dieser Liste beschrieben).

6 Es wird eine Meldung mit dem Vorschlag angezeigt, Microsoft SQL Express 2008 R2 zu installieren. Klicken Sie im Meldungsfenster auf **Ja**. Die Installation von Microsoft SQL Express 2008 R2 wird gestartet. Nach Abschluss der Installation wird die Seite mit der Lizenzvereinbarung von ViPNet Network Manager eingeblendet.

7 Machen Sie sich mit den Lizenzbedingungen vertraut. Falls Sie mit den Bedingungen einverstanden sind, aktivieren Sie das Kontrollkästchen **Ich akzeptiere diese Lizenzvereinbarung** und klicken auf **Weiter**. Wenn Sie die Bedingungen nicht akzeptieren, ist das Fortsetzen der Installation von ViPNet Network Manager nicht möglich.

8 Zum Starten der Installation von ViPNet Network Manager klicken Sie auf **Jetzt installieren**.



Hinweis. Klicken Sie auf **Einstellungen**, wenn Sie den Installationsordner des Programms ändern, Benutzerdaten ergänzen oder den Programmordner im Menü **Start** festlegen wollen.

9 Nach Abschluss der Installation wird eine Meldung über die erfolgreich durchgeführte Installation angezeigt. Klicken Sie im Meldungsfenster auf **Schließen**.

10 Wenn eine Aufforderung zum Nestart des Computers erscheint, klicken Sie auf **Ja**.

Bevor Sie ViPNet Client- oder ViPNet Coordinator-Software auf dem Manager-Arbeitsplatz installieren, sollten Sie die Struktur des ViPNet Netzwerks und die Schlüsseldistributionen für die einzelnen Netzwerkknoten erstellen (s. Arbeit beginnen. Erstellen der ViPNet Struktur auf S. 83).

Installation von ViPNet Client oder ViPNet Coordinator auf dem Manager-Arbeitsplatz

Für die Installation von ViPNet Client oder ViPNet Coordinator auf dem Manager-Arbeitsplatz werden folgende Komponenten benötigt:

- Das ViPNet VPN-Installationsprogramm.
- Die Schlüsseldistribution (Datei `*.dst`) für den Netzwerkknoten mit dem Manager-Arbeitsplatz.
- Das Benutzerpasswort für diesen Netzwerkknoten.



Achtung! Stellen Sie vor der Installation der ViPNet Client- oder ViPNet Coordinator-Software sicher, dass der Computer den Systemanforderungen entspricht (s. ViPNet Client auf S. 23).

Zum Installieren von ViPNet Client oder ViPNet Coordinator:

1 Schließen Sie alle Anwendungen.

2 Starten Sie das Installationsprogramm von ViPNet VPN.

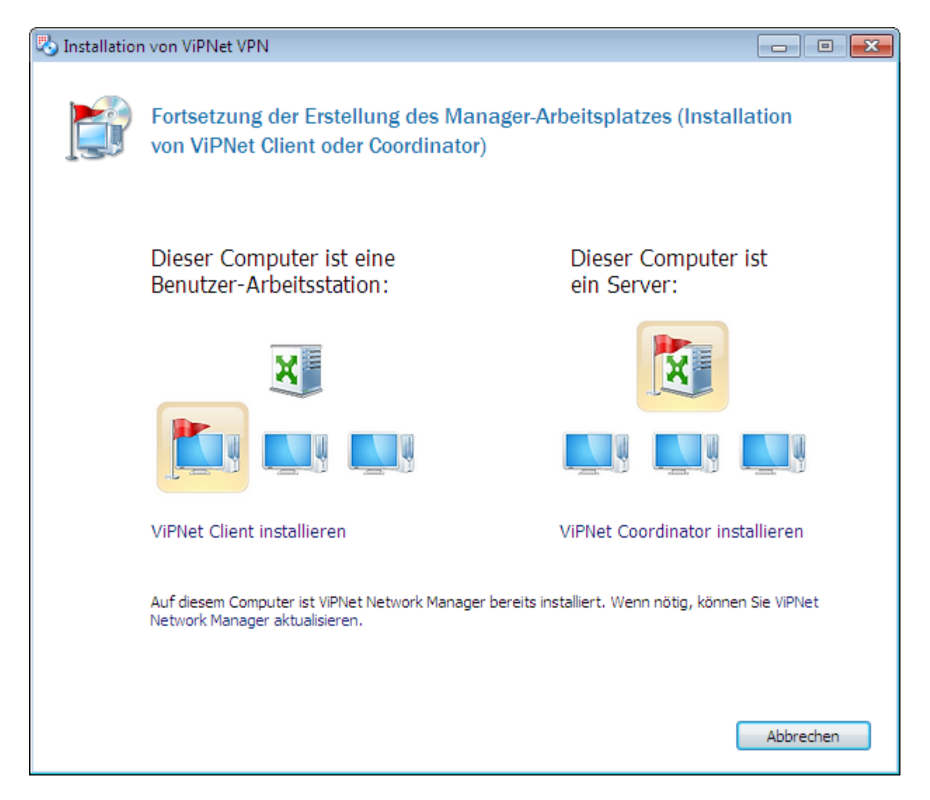


Abbildung 14. Fortsetzung der Erstellung des Manager-Arbeitsplatzes

3 Klicken Sie auf den entsprechenden Link, um ViPNet Client oder ViPNet Coordinator zu installieren.

4 Installieren Sie die Software ViPNet Client oder ViPNet Coordinator, indem Sie den Anweisungen folgen, die in den entsprechenden Abschnitten aufgeführt sind:

- Installation von ViPNet Coordinator auf ViPNet Netzwerkserver (auf S. 57)
- Einrichtung der Benutzerarbeitsplätze im ViPNet Netzwerk (auf S. 59)

Der Manager-Arbeitsplatz ist nun einsatzbereit.

Installation von ViPNet Coordinator auf ViPNet Netzwerkserver

Für die Installation von ViPNet Coordinator auf Computer, die als Server im ViPNet Netzwerk eingesetzt werden sollen, werden folgende Komponenten benötigt:

- Das Installationsprogramm von ViPNet VPN.
- Die *.dst-Dateien mit den Schlüsseldistributionen für den Coordinator. Die *.dst-Datei können Sie im ViPNet Network Manager in der Registerkarte Schlüssel **Schlüssel** des entsprechenden Coordinators kopieren.
- Das Benutzerpasswort für den Coordinator. Das Benutzerpasswort können Sie ebenfalls im ViPNet Network Manager in der Registerkarte **Schlüssel** des entsprechenden Coordinator finden.



Achtung! Stellen Sie vor der Installation der ViPNet Coordinator-Software sicher, dass der Computer den Systemanforderungen entspricht (s. ViPNet Coordinator auf S. 22).

Zum Installieren von ViPNet Coordinator:

1. Schließen Sie alle Anwendungen.
2. Starten Sie das Installationsprogramm von ViPNet VPN.
3. Klicken Sie **Installation der ViPNet VPN Software-Module** den zweiten Link **Installation der Software-Module auf den Servern (Coordinatoren) des ViPNet Netzwerkes (Installation von ViPNet Coordinator)**.

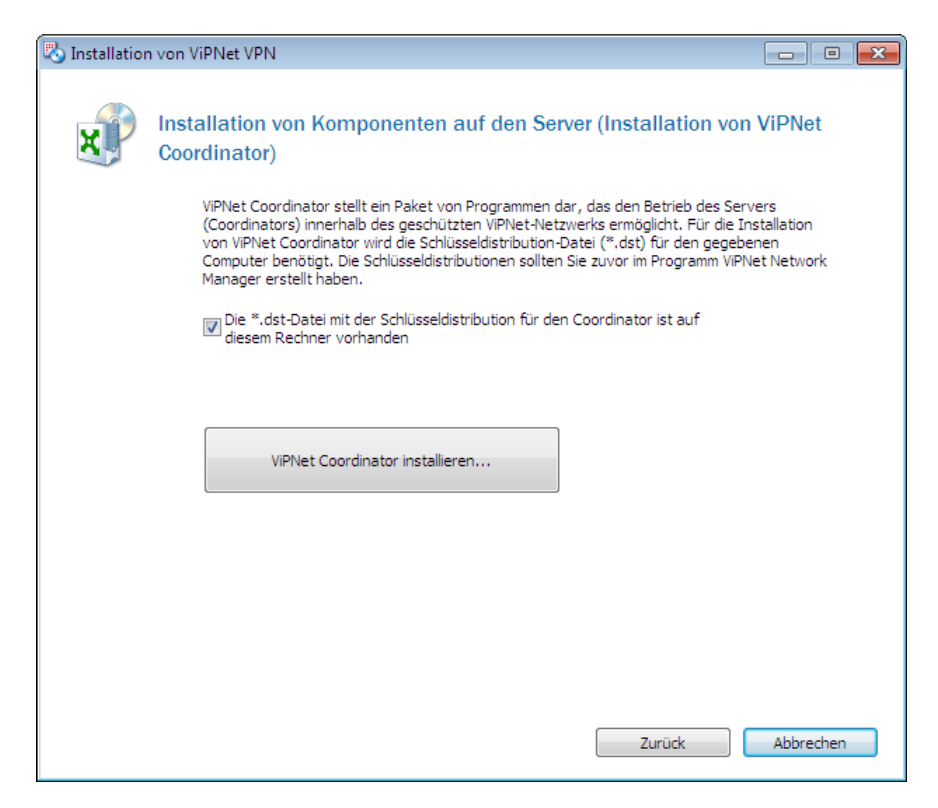


Abbildung 15. ViPNet Coordinator installieren

4 Aktivieren Sie das Kontrollkästchen **Die DST-Datei mit der Schlüsseldistribution für den Coordinator ist auf diesem Rechner vorhanden**.

5 Wenn der Computer nach der Installation des Programms ViPNet Coordinator neu gestartet werden soll, aktivieren Sie das Kontrollkästchen **Bei Remoteinstallation das Betriebssystem automatisch neu starten**.

6 Klicken Sie auf die Schaltfläche **ViPNet Coordinator installieren**. Es wird der Assistent **Installation von ViPNet Coordinator** gestartet.

   Folgen Sie den Anweisungen des Assistenten.

7 Doppelklicken Sie auf die *.dst-Datei, um die Schlüsseldistribution zu installieren, und folgen den Anweisungen des Assistenten.

8 Starten Sie das Programm ViPNet Coordinator und führen die Konfiguration des Programms durch (s. Arbeit mit dem Programm ViPNet Client für Windows auf S. 215).

Einrichtung der Benutzerarbeitsplätze im ViPNet Netzwerk

Für die Installation von ViPNet Client auf Computer, die als Benutzerarbeitsplätze im ViPNet Netzwerk eingesetzt werden sollen, werden folgende Komponenten benötigt:

- Das Installationsprogramm von ViPNet VPN.
- Die *.dst-Dateien mit den Schlüsseldistributionen für den Client. Die *.dst-Datei können Sie im Programm ViPNet Network Manager in der Registerkarte **Schlüssel** des entsprechenden Clients kopieren.
- Das Benutzerpasswort finden Sie auf dem Client im Programm ViPNet Network Manager auf der Registerkarte **Schlüssel** oder in der Datei `ViPNet.txt`, die sich im gleichen Ordner wie die gespeicherten Schlüsseldistributionen des Knotens befindet.



Achtung! Stellen Sie vor der Installation der ViPNet Client-Software sicher, dass der Computer den Systemanforderungen entspricht (s. ViPNet Client auf S. 23).

Zum Installieren von ViPNet Client:

1. Schließen Sie alle Anwendungen.
2. Starten Sie das Installationsprogramm von ViPNet VPN.
3. Klicken Sie auf der Seite **Installation der ViPNet VPN Software-Module** auf den dritten Link **Erstellen des Benutzer-Arbeitsplatzes (Installation von ViPNet Client)**.

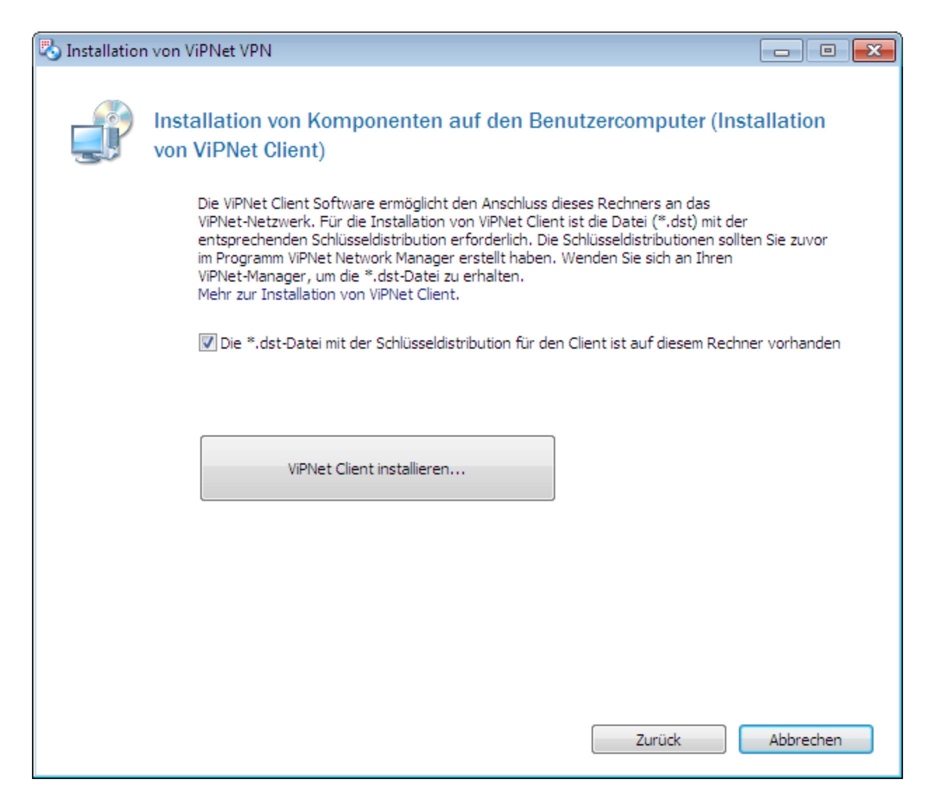


Abbildung 16. ViPNet Client installieren

4 Aktivieren Sie das Kontrollkästchen **Die DST-Datei mit der Schlüsseldistribution für den Client ist auf diesem Rechner vorhanden**.

5 Wenn der Computer nach der Installation des Programms ViPNet Client neu gestartet werden soll, aktivieren Sie das Kontrollkästchen **Bei Remoteinstallation das Betriebssystem automatisch neu starten**.

6 Klicken Sie auf die Schaltfläche **ViPNet Client installieren**. Es wird der Assistent **Installation von ViPNet Client** gestartet.

Folgen Sie den Anweisungen des Assistenten.

7 Doppelklicken Sie auf die *.dst-Datei, um die Schlüsseldistribution zu installieren, und folgen den Anweisungen des Assistenten.

8 Starten Sie das Programm ViPNet Client und führen die Konfiguration des Programms durch.

Remote-Installation von ViPNet Client und ViPNet Coordinator

Wenn ViPNet Software auf einem entfernten Rechner installiert werden soll, kann der Administrator des ViPNet Netzwerks die Installation per Remotezugriff durchführen, indem er sich über das RDP-Protokoll zum entfernten Computer verbindet.

Führen Sie die folgenden Schritte aus, um eine Remoteinstallation von ViPNet Software mit anschließendem automatischen Neustart des entfernten Computers durchzuführen:

1 Stellen Sie mit Hilfe des Windows-Standardprogramms „Remotedesktopverbindung" eine Verbindung zum entfernten Computer her, auf welchem die ViPNet Software installiert werden soll.



Achtung! Auf dem entfernten Computer sollten Remotedesktopverbindungen erlaubt sein. Für die Verbindung sollte auf dem Remotecomputer ein Windows-Benutzerkonto verwendet werden, das über Administratorrechte verfügt und durch ein Passwort geschützt ist.

2 Kopieren Sie das Installationsprogramm von ViPNet VPN und die Schlüsseldistribution für den Netzwerkknoten (Datei mit der Erweiterung `.dst`) auf den entfernten Computer.

3 Starten Sie während der Fernzugriffssitzung das Installationsprogramm von ViPNet VPN. Es wird der Installationsassistent von ViPNet VPN geöffnet.

Ausführliche Informationen über die Installation von ViPNet Client und ViPNet Coordinator mit Hilfe eines Assistenten s. Abschnitte Einrichtung der Benutzerarbeitsplätze im ViPNet Netzwerk (auf S. 59) und Installation von ViPNet Coordinator auf ViPNet Netzwerkserver (auf S. 57).

4 Wählen Sie das Programm für die Installation aus und aktivieren auf der folgenden Seite des Assistenten das Kontrollkästchen **Die *.dst-Datei mit der Schlüsseldistribution für den Client (Coordinator) ist auf diesem Rechner vorhanden**.

5 Klicken Sie auf die Schaltfläche **ViPNet Client installieren** oder **ViPNet Coordinator installieren**.

6 Geben Sie mit Hilfe des Assistenten die benötigten Installationsparameter für das ViPNet Programm an.

7 Zum Installieren der ViPNet Schlüssel auf dem entfernten Computer, doppelklicken Sie auf die Schlüsseldistributionsdatei und klicken im Fenster **ViPNet Schlüsselinstallation** auf die Schaltfläche **Schlüssel installieren**.

Der entfernte ViPNet Netzwerkknoten ist nun einsatzbereit.

Upgrade von ViPNet VPN Version 3.x auf Version 4.x

Vorgehensweise beim Upgrade

Führen Sie folgende Schritte aus, um die Software ViPNet VPN der Version 3.x auf die Version 4.x zu aktualisieren. Ein Upgrade des Programms ViPNet Network Manager von Version 2.x auf Version 4.x ist nicht möglich. Falls ViPNet Network Manager 2.x verwendet wird, aktualisieren Sie das Programm zunächst auf Version 3.x. Führen Sie anschließend das Upgrade auf Version 4.x durch.



Achtung! Es sollte beachtet werden, dass nach einem Upgrade von ViPNet Network Manager auf die Version 4.x im Programm alle Einschränkungen einer nicht registrierten Version wirksam werden, auch wenn die vorhergehende Version des Programms registriert war (s. Einschränkung der Funktionalität nach Upgrade des Programms ViPNet Network Manager auf die Version 4.x auf S. 65).

Tabelle 5. ViPNet VPN auf Version 4.x aktualisieren

	Aktion	Verweis
☐	Wenden Sie sich an einen Vertreter der Infotecs GmbH und fordern eine Seriennummer für die Software ViPNet VPN Version 4.x an.	Kontakt (auf S. 25)
☐	Aktualisieren Sie die Software ViPNet Coordinator und ViPNet Client auf allen Coordinatoren und Clients. Führen Sie dazu einen der folgenden Schritte aus: • Versenden Sie aus dem Programm ViPNet Network Manager die Software ViPNet Client und ViPNet Coordinator Version 4.x an die Netzwerkknoten. • Starten Sie auf jedem Netzwerkknoten das Installationsprogramm von ViPNet VPN Version 4.x und klicken im Fenster **ViPNet VPN Setup** auf die Schaltfläche **ViPNet Coordinator aktualisieren** oder **ViPNet Client aktualisieren**.	Versenden von ViPNet Softwareupdates (auf S. 149) Installation von ViPNet Coordinator auf ViPNet Netzwerkserver (auf S. 57) Einrichtung der Benutzerarbeitsplätze im ViPNet Netzwerk (auf S. 59)
☐	Wenn die vorhergehende Version von ViPNet Network Manager registriert war, sichern Sie die Datei `offmanager.brg`, die sich im Installationsordner von ViPNet Network Manager befindet.	Registrierungsdaten speichern (auf S. 81)

	Aktion	Verweis
☐	Schließen Sie alle Vorgänge ab, die in Zusammenhang mit Partnernetzwerk-Verbindungen stehen: Aufbau von Verbindungen zu neuen Partnernetzwerken, Empfang und Versand von Partnernetzwerk-Daten.	Partnernetzwerk-Verbindungen (auf S. 165)
☐	Aktualisieren Sie das Programm ViPNet Network Manager auf dem Manager-Arbeitsplatz.	Upgrade von ViPNet Network Manager auf Version 4.x (auf S. 63)
☐	Damit Sie die Vollversion von ViPNet Network Manager benutzen können, sollten Sie das Programm mit Hilfe der Seriennummer für die Version 4.x registrieren.	Registrierung von ViPNet Network Manager (auf S. 70)
☐	Versenden Sie die Schlüsselupdates an die Netzwerkknoten.	Versenden der Schlüssel-Updates (auf S. 145)



Tipp. Wir empfehlen, die Liste auszudrucken, und die einzelnen Schritte nach ihrer Durchführung zu markieren.

Upgrade von ViPNet Network Manager auf Version 4.x



Achtung! Ein Upgrade des Programms ViPNet Network Manager von Version 2.x auf Version 4.x ist nicht möglich. Falls ViPNet Network Manager 2.x verwendet wird, aktualisieren Sie das Programm zunächst auf Version 3.x. Führen Sie anschließend das Upgrade auf Version 4.x durch.

Führen Sie die folgenden Schritte aus, um ViPNet Network Manager der Version 3.x auf die Version 4.x zu aktualisieren:

1 Es wird empfohlen, vor Beginn der Aktualisierung die Datei `offmanager.brg` aus dem Installationsordner von ViPNet Network Manager zu sichern. Diese Datei kann benötigt werden, wenn Sie sich für eine Rückkehr zur Version 3.x entscheiden (s. Rückkehr zur Version 3.x auf S. 66).

2 Schließen Sie alle Vorgänge ab, die in Zusammenhang mit Partnernetzwerk-Verbindungen stehen: Aufbau von Verbindungen zu neuen Partnernetzwerken, Empfang und Versand von Partnernetzwerk-Daten (s. Partnernetzwerk-Verbindungen auf S. 165).

3 Falls ViPNet Network Manager Version 2.x verwendet wird, aktualisieren Sie das Programm zuerst auf Version 3.x.

4 Führen Sie die folgenden Schritte aus, um ViPNet Network Manager auf Version 4.x zu aktualisieren:

4.1 Starten Sie auf dem Administrator-Rechner das Installationsprogramm von ViPNet VPN Version 4.x und klicken im Fenster **ViPNet VPN Setup** auf die Schaltfläche **ViPNet Network Manager aktualisieren**.

4.2 Starten Sie das Programm ViPNet Network Manager. Beim Start wird eine Meldung eingeblendet, dass das Programm nicht registriert ist.

Wählen Sie im Meldungsfenster die Option **ViPNet Network Manager registrieren** und registrieren das Programm (s. Registrierung von ViPNet Network Manager auf S. 70).



Achtung! Wenn Sie ViPNet Network Manager nach der Aktualisierung auf Version 4.x nicht registrieren, dann gelten im Programm alle Einschränkungen der Demo-Version, und zwar auch dann wenn die vorherige Version des Programms registriert war (s. Einschränkung der Funktionalität nach Upgrade des Programms ViPNet Network Manager auf die Version 4.x auf S. 65).

5 Versenden Sie Schlüsselupdates (s. Versenden der Schlüssel-Updates auf S. 145) an die Netzwerkknoten.

Beim erstmaligen Versand der Schlüssel nach der Aktualisierung von ViPNet Network Manager kann die Liste der Netzwerkknoten für den Versand nicht geändert werden. Das Update wird an alle Knoten weitergeleitet. Der Zeitpunkt des Inkrafttretens von Änderungen kann frühestens eine Stunde ab dem aktuellen Zeitpunkt liegen.

6 Die neue Version von ViPNet Network Manager ist nun einsatzbereit.

Upgrade von ViPNet Network Manager und Übertragung des Programms auf einen neuen Computer

Wenn auf der Arbeitsstation des ViPNet Administrators das Programm ViPNet Network Manager aktualisiert und der Computer gegen einen neuen ausgetauscht werden soll, dann führen Sie alle Tasks aus der weiter unten aufgeführten Liste aus.

	Aktion	Verweis
☐	Führen Sie auf dem alten Computer das Upgrade von ViPNet Network Manager durch.	Upgrade von ViPNet Network Manager auf Version 4.x (auf S. 63)
☐	Exportieren Sie nach dem Upgrade von ViPNet Network Manager auf dem alten Computer die Konfiguration des Programms in eine Datei.	Export der Konfiguration (auf S. 161)
☐	Installieren Sie ViPNet Network Manager auf dem neuen Computer.	Installation von ViPNet Network Manager (auf S. 53)

	Aktion	Verweis
☐	Führen Sie auf dem neuen Computer den Import der ViPNet Network Manager-Konfiguration aus der vorher erstellten Datei durch.	Import der Konfiguration (auf S. 161)
☐	Trennen Sie den alten Computer vom Netzwerk oder deinstallieren dort das Programm ViPNet Client.	
☐	Speichern Sie auf dem neuen Computer im Programm ViPNet Network Manager eine Schlüsseldistribution für den Manager-Arbeitsplatz ab.	Versand und Speicherung der Netzwerkknotenschlüssel (auf S. 147)
☐	Installieren Sie auf dem neuen Computer das Programm ViPNet Client oder ViPNet Coordinator.	Installation von ViPNet Client oder ViPNet Coordinator auf dem Manager-Arbeitsplatz (auf S. 55)
☐	Installieren Sie auf dem neuen Computer die vorher erstellten Schlüssel für den Manager-Arbeitsplatz.	



Tipp. Wir empfehlen, die Liste auszudrucken, und die einzelnen Schritte nach ihrer Durchführung zu markieren.

Einschränkung der Funktionalität nach Upgrade des Programms ViPNet Network Manager auf die Version 4.x

Wenn vor dem Upgrade auf die Version 4.x das Programm ViPNet Network Manager bereits registriert war, wird das Programm nach dem Upgrade wieder als nicht registrierte Version geführt. Die Funktionalität des Programms wird eingeschränkt (s. Einschränkungen der kostenlosen Version auf S. 47).

Die vor dem Upgrade eingerichteten Netzwerkknoten, getunnelten Verbindungen und Partnernetzwerke bleiben erhalten. Beim Arbeiten mit ViPNet Network Manager können Sie jedoch mit folgenden Einschränkungen konfrontiert werden:

- Das Programm ViPNet Network Manager kann nur innerhalb eines Zeitraums von 60 Tagen verwendet werden.
- Es können keine zusätzlichen Netzwerkknoten eingerichtet werden.
- Es können keine Partnernetzwerk-Verbindungen zu bestehenden Partnernetzwerken aufgebaut werden. Der Austausch von Partnernetzwerk-Informationen (s. Partnernetzwerk-Verbindungen auf S. 165) wird nicht möglich sein.

- Nach Versenden der Schlüsselupdates an die Netzwerkknoten wird die Nutzungsdauer der Software ViPNet Client und ViPNet Coordinator auf diesen Knoten ebenfalls eingeschränkt.

Registrieren Sie das Programm (s. Registrierung von ViPNet Network Manager auf S. 70), um die funktionellen Einschränkungen der Software ViPNet Network Manager wieder zu beseitigen.

Rückkehr zur Version 3.x

Wenn Sie nach einem Upgrade des Programms ViPNet Network Manager auf die Version 4.x wieder zur vorhergehenden Version zurückkehren möchten, führen Sie folgende Schritte aus:

1. Deinstallieren Sie das Programm ViPNet Network Manager 4.x auf dem Administrator-Computer.
2. Installieren Sie das Programm ViPNet Network Manager Version 3.x.
3. Wenn das Programm ViPNet Network Manager Version 3.x bereits registriert war, führen Sie eine der folgenden Aktionen aus:
    - Wenn Sie vor dem Upgrade auf Version 4.x die Datei `offmanager.brg` gesichert haben, dann kopieren Sie diese Datei nun in den Installationsordner von ViPNet Network Manager. Das Programm wird registriert.
    - Wenn Sie die Datei `offmanager.brg` nicht gesichert haben, registrieren Sie das Programm neu (s. Registrierung von ViPNet Network Manager auf S. 70), indem Sie die vorhandene Seriennummer von ViPNet VPN Version 3.x verwenden.

Verlegen des Manager-Arbeitsplatzes auf einen anderen Netzwerkknoten

Bei der Arbeit mit ViPNet Network Manager kann sich die Notwendigkeit ergeben, den Manager-Arbeitsplatz auf einen anderen Computer (zum Beispiel, wenn ein veralteter Computer gegen einen neuen ausgetauscht werden soll) oder auf einen anderen Netzwerkknoten zu verlegen (zum Beispiel, wenn als Manager-Arbeitsplatz ein Coordinator festgelegt wurde, das ViPNet Netzwerk aber so gewachsen ist, dass ein eigener Client für den Manager-Arbeitsplatz bereitgestellt werden soll). Im Programm ViPNet Network Manager gibt es folgende Möglichkeiten zur Übertragung des Manager-Arbeitsplatzes:

- Übertragung des Manager-Arbeitsplatzes auf einen anderen Netzwerkknoten, falls das ViPNet Netzwerk noch nicht vollständig installiert ist. Legen Sie in diesem Fall den benötigten Knoten als Manager-Arbeitsplatz fest (s. Zuweisung des Manager-Arbeitsplatzes an einen anderen Knoten auf S. 136) und setzen die Installation des ViPNet Netzwerks fort.
- Übertragung des Manager-Arbeitsplatzes auf einen anderen Computer ohne Wechsel des Netzwerkknotens. Führen Sie in diesem Fall die im Abschnitt Upgrade von ViPNet Network Manager und Übertragung des Programms auf einen neuen Computer (auf S. 64) beschriebenen Aktionen durch.
- Übertragung des Manager-Arbeitsplatzes mit allen erforderlichen Informationen über das eingerichtete ViPNet Netzwerk und den Programmeinstellungen von ViPNet Network Manager auf einen anderen Netzwerkknoten. Führen Sie in diesem Fall die Schritte durch, die in der Tabelle unten aufgeführt sind.



Hinweis. Der Manager-Arbeitsplatz kann auf folgende Netzwerkknoten installiert werden:

- auf beliebige Clients;
- auf Coordinatoren mit dem Betriebssystems Windows.

Tabelle 6. Vorgehensweise bei der Verlegung des Manager-Arbeitsplatzes auf einen anderen Knoten

	Aufgabe	Link
☐	Legen Sie einen anderen Netzwerkknoten (Client oder Coordinator) als Manager-Arbeitsplatz fest.	Zuweisung des Manager-Arbeitsplatzes an einen anderen Knoten (auf S. 136)

	Aufgabe	Link
☐	Exportieren Sie die Konfiguration des ViPNet Netzwerks und übertragen die Datei der Sicherungskopie `*.rps` auf den neuen Administrator-Netzwerkknoten.	Export der Konfiguration (auf S. 161)
☐	Installieren Sie das Programm ViPNet Network Manager auf den neuen Manager-Arbeitsplatz.	Installation von ViPNet Network Manager (auf S. 53)
☐	Importieren Sie die Datei der Sicherungskopie `*.rps` im Programm ViPNet Network Manager. Dabei werden alle Lizenz- und Registrierungsdaten für das Programm ViPNet Network Manager ebenfalls importiert.	Import der Konfiguration (auf S. 161)
☐	Speichern Sie die Schlüssel und übergeben diese manuell auf eine sichere Art an die Benutzer der Netzwerkknoten.	Speichern der Schlüsseldistributionen (auf S. 142)
☐	Wenn Partnernetzwerk-Verbindungen eingerichtet waren, erstellen Sie eine neue Partnernetzwerk-Information und leiten diese manuell an die Administratoren der Partnernetzwerke auf eine sichere Art weiter.	Initiierung der Partnernetzwerk-Verbindung (auf S. 169)
☐	Installieren Sie das Programm ViPNet Client oder ViPNet Coordinator sowie die Schlüssel auf dem neuen Manager-Arbeitsplatz.	Installation von ViPNet Client oder ViPNet Coordinator auf dem Manager-Arbeitsplatz (auf S. 55)
☐	Installieren Sie die Schlüssel auf den Clients und Coordinatoren des eigenen ViPNet Netzwerks.	



Tipp. Wir empfehlen, die Liste auszudrucken, und die einzelnen Schritte nach ihrer Durchführung zu markieren.

Deinstallation von ViPNet VPN

Es wird empfohlen, vor einer Deinstallation des Programms ViPNet Network Manager, das für die Steuerung eines funktionsfähigen ViPNet Netzwerks verwendet wird, eine Sicherungskopie der Konfiguration von ViPNet Network Manager zu erstellen (s. Export der Konfiguration auf S. 161). Wenn eine erneute Installation des Programms ViPNet Network Manager erforderlich wird, können Sie mit Hilfe der Sicherungskopie der Konfiguration die Parameter Ihres ViPNet Netzwerks, die Registrierungsdaten der Software und andere Daten schnell wiederherstellen.

Führen Sie zum Deinstallieren der Software ViPNet Network Manager die folgenden Schritte aus:

1 Verwenden Sie das Betriebssystem Windows 7 oder eine frühere Version, wählen Sie im Menü **Start** den Eintrag **Alle Programme** > **ViPNet** > **ViPNet Network Manager** > **ViPNet Network Manager deinstallieren**.

Verwenden Sie das Betriebssystem Windows 8 oder eine spätere Version, öffnen Sie die Apps-Liste auf der Startseite und wählen den Eintrag **ViPNet** > **ViPNet Network Manager deinstallieren**.

2 Wählen Sie im eingeblendeten Fenster des Installationsassistenten von ViPNet Network Manager das Optionsfeld **Alle Komponenten entfernen** und klicken dann auf **Weiter**.

3 Aktivieren Sie auf der nachfolgenden Assistentenseite bei Bedarf das Kontrollkästchen **Benutzerdaten löschen** und klicken dann auf **Deinstallieren**.

Bei der Deinstallation von ViPNet Network Manager wird die Software Microsoft SQL Server nicht deinstalliert. Diese Software wird für die Steuerung der Datenbank von ViPNet Network Manager verwendet. Wenn außerdem das Kontrollkästchen **Benutzerdaten löschen** beim Deinstallieren nicht aktiviert wurde, dann wird die Datenbank von ViPNet Network Manager ebenfalls nicht gelöscht. Wenn Sie das Programm ViPNet Network Manager erneut auf dem Computer installieren, wird das Programm versuchen, die bestehende Datenbank zu verwenden, und das früher erstellte ViPNet Netzwerk wird beibehalten.

Wenn Sie sämtliche Daten über das ViPNet Netzwerk löschen und die Software Microsoft SQL Server deinstallieren möchten, dann führen Sie die folgenden Schritte aus:

1 Löschen Sie alle Daten in den Ordnern `C:\ProgramData\InfoTeCS\ViPNet Network Manager` und `C:\Users\<Benutzername>\AppData\Roaming\InfoTeCS\ViPNet Network Manager`.

2 Deinstallieren Sie mit Hilfe der Systemsteuerung (Eintrag „Software“) die Software Microsoft SQL Server und die Komponente Microsoft SQL Server Native Client.



Achtung! Wenn Sie vorhaben, das Programm ViPNet Network Manager zu einem späteren Zeitpunkt wieder auf dem gleichen Computer zu installieren, dann sollte bei der Deinstallation von Microsoft SQL Server auch die Komponente Microsoft SQL Server Native Client deinstalliert werden. Wenn diese Komponente nicht deinstalliert wird, wird eine spätere Installation von ViPNet Network Manager nicht möglich sein.

3

Registrierung von ViPNet Network Manager

Vor der Registrierung von ViPNet Network Manager

Warum ViPNet Network Manager registriert werden sollte

Nach der Installation von ViPNet Network Manager arbeitet das Programm zunächst als Free Edition (s. Einschränkungen der kostenlosen Version auf S. 47). ViPNet Network Manager kann jederzeit registriert werden. Danach steht der volle Funktionsumfang des Programms ohne zeitliche Einschränkungen zur Verfügung.

Folgende Vorgangsweise wird empfohlen:

- installieren Sie ViPNet Network Manager und nutzen die nicht registrierte Version des Programms, um die Möglichkeiten und Vorteile des Produkts kennenzulernen;
- registrieren Sie Ihre Kopie von ViPNet Network Manager.

Registrierung starten



Hinweis. Wenn ViPNet Network Manager erneut auf einem Computer installiert wurde, auf dem es bereits registriert war, können Sie die in der Datei *.brg gespeicherten Registrierungsdaten benutzen (s. Registrierungsdaten speichern auf S. 81).

Wenn Sie Änderungen an der Konfiguration des Computers vorgenommen haben, auf dem ViPNet Network Manager, im Einsatz ist, lesen Sie bitte den Abschnitt Wenn sich die Konfiguration Ihres Computers geändert hat (auf S. 82).

Führen Sie folgende Schritte aus, um ViPNet Network Manager zu registrieren:

1 Klicken Sie im Hauptfenster von ViPNet Network Manager im Menü **Hilfe** auf den Eintrag **Registrierung**.

2 Es wird der Assistent **ViPNet Network Manager Registrierung** gestartet.



Abbildung 17. Registrierungs-Assistent für ViPNet Network Manager

3 Wenn Sie zu diesem Zeitpunkt:

- ViPNet Network Manager noch nicht gekauft haben, wählen Sie die Option **Kauf (wenn Sie noch keine Seriennummer haben)** (s. Seriennummer anfordern auf S. 73).



Hinweis. Wenn Sie ViPNet Network Manager auf einer CD erworben haben, dann verfügen bereits über eine Seriennummer (diese ist gemeinsam mit der CD im Paket enthalten), und können unmittelbar zur Anfrage des Registrierungscodes übergehen (siehe unten).

- ViPNet Network Manager bereits gekauft haben und über eine Seriennummer verfügen, wählen Sie **Registrierungsanfrage (wenn Sie bereits eine Seriennummer haben)** (s. Registrierungscode anfordern auf S. 74).



Hinweis. Wenn Sie eine Registrierungsanfrage über das Internet gesendet haben, erfolgt die Registrierung von ViPNet Network Manager automatisch ohne weitere Mitwirkung Ihrerseits.

4 ViPNet Network Manager bereits gekauft und einen Registrierungscode erhalten haben, wählen Sie **Registrieren** (s. ViPNet Network Manager registrieren auf S. 80).

Seriennummer anfordern

Zum Anfordern einer Seriennummer:

1 Wählen Sie im Assistentenfenster **ViPNet Network Manager Registrierung** die Option **Kauf (wenn Sie noch keine Seriennummer haben)** und klicken auf **Weiter**.

   In Ihrem Browser wird die Website für die Bestellung von ViPNet Produkten von Infotecs geöffnet. Erwerben Sie ViPNet Network Manager über die Website. Sie erhalten die Seriennummer per E-Mail.

2 Kehren Sie nach Erhalt der Seriennummer zum Assistenten **ViPNet Network Manager Registrierung** (s. Registrierung starten auf S. 71) zurück und führen die Anfrage des Registrierungscodes durch (s. Registrierungscode anfordern auf S. 74).

Registrierungscode anfordern

Zum Anfordern eines Registrierungscodes für ViPNet Network Manager:

1 Wählen Sie im Assistentenfenster **ViPNet Network Manager Registrierung** die Option **Registrierungsanfrage (wenn Sie bereits eine Seriennummer haben)** und klicken auf **Weiter**.

2 Wählen Sie im Fenster **Möglichkeiten der Registrierungsanfrage** die für Sie passende Option aus. Aktivieren Sie dazu eines der folgenden Optionsfelder:

- **Über das Internet (online)** (s. Registrierungsanfrage über das Internet auf S. 74).
- **Via E-Mail** (s. Registrierungsanfrage via E-Mail auf S. 77).
- **Per Telefon** (s. Registrierungsanfrage per Telefon auf S. 78).

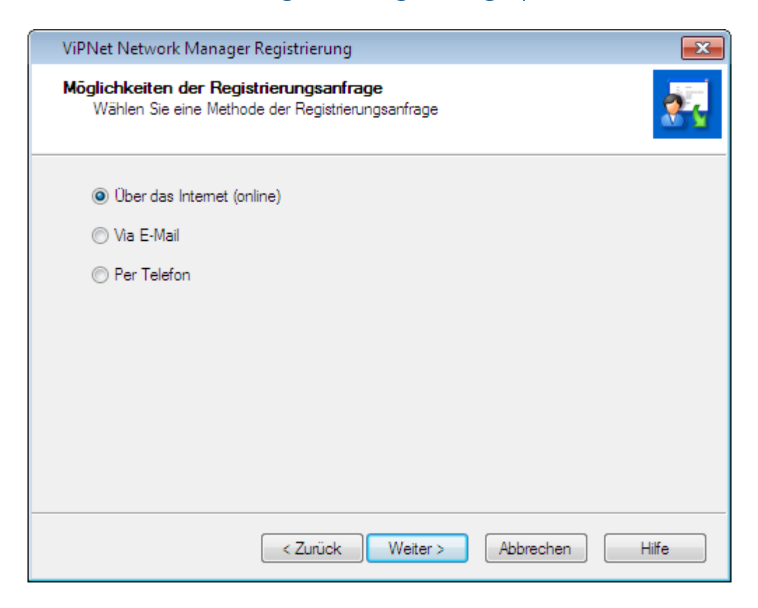


Abbildung 18. Methode der Registrierungsanfrage wählen

3 Klicken Sie auf die Schaltfläche **Weiter**.

Registrierungsanfrage über das Internet



Achtung! Für diese Registrierungsmöglichkeit ist ein Internet-Zugang erforderlich.

Wenn Sie die Registrierungsoption **Über das Internet (online)** gewählt haben, wird das Fenster **Registrierungsdaten** eingeblendet.

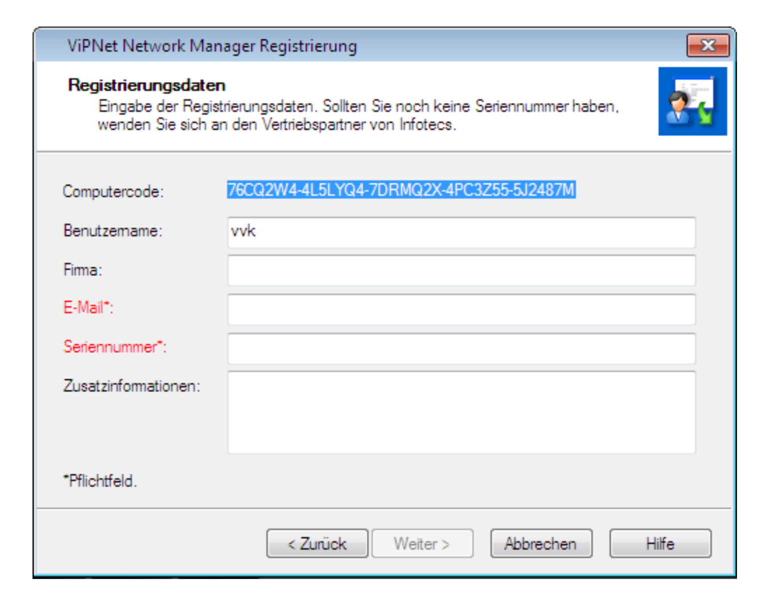


Abbildung 19. Fenster zur Eingabe von Registrierungsdaten

Führen Sie im Fenster **Registrierungsdaten** folgende Schritte aus:

1 Geben Sie im Feld **Seriennummer** die Seriennummer ein.



Hinweis. Wenn Sie über keine Seriennummer verfügen, fordern Sie diese zunächst an (s. Seriennummer anfordern auf S. 73).

Wenn Sie die Seriennummer zu einem früheren Zeitpunkt bereits eingegeben haben, so erscheint diese hier automatisch.

2 Geben Sie im Feld **Benutzername** Ihren Namen ein. Dieser wird für die Herausgabe der Lizenz und für die Ansprache verwendet. Dieses Feld muss nicht ausgefüllt werden. Standardmäßig wird im Feld **Benutzername** der Name eingeblendet, den Sie während der Installation von ViPNet Network Manager angegeben haben.

3 Geben Sie im Feld **Firma** den Namen Ihrer Firma ein. Dieses Feld muss nicht ausgefüllt werden. Standardmäßig wird im Feld **Firma** der Firmenname eingeblendet, den Sie während der Installation von ViPNet Network Manager angegeben haben.

4 Geben Sie im Feld **E-Mail** ihre E-Mail-Adresse ein. Diese wird in besonderen Fällen für eine Kontaktaufnahme genutzt.



Achtung! Ihre E-Mail-Adresse wird von uns weder verkauft noch weiterverbreitet. Die Firma „Infotecs nimmt den Schutz Ihrer persönlichen Daten sehr ernst und trifft alle Maßnahmen zur Verhinderung von unberechtigtem Zugriff auf Daten und unerlaubter Weiterleitung von Informationen.

5 Im Feld **Zusatzinformationen** können Sie beliebige zusätzliche Anmerkungen angeben, zum Beispiel Ihre Kontaktdaten, Meldungen über mögliche Probleme oder Anregungen, die sich auf ViPNet Software beziehen.

Im Feld **Computercode** wird ein Code eingeblendet, der Ihren Computer eindeutig identifiziert. Der Wert in diesem Feld kann nicht geändert werden.

6 Klicken Sie auf die Schaltfläche **Weiter**. Es wird ein Fenster geöffnet, das den Status der Registrierungsanfrage anzeigt. Hier wird die Zeit seit dem Beginn des laufenden Versuchs einer Registrierungsanfrage hochgezählt. Beachten Sie, dass für den Aufbau einer Verbindung nicht mehr als 3 Minuten veranschlagt sind.

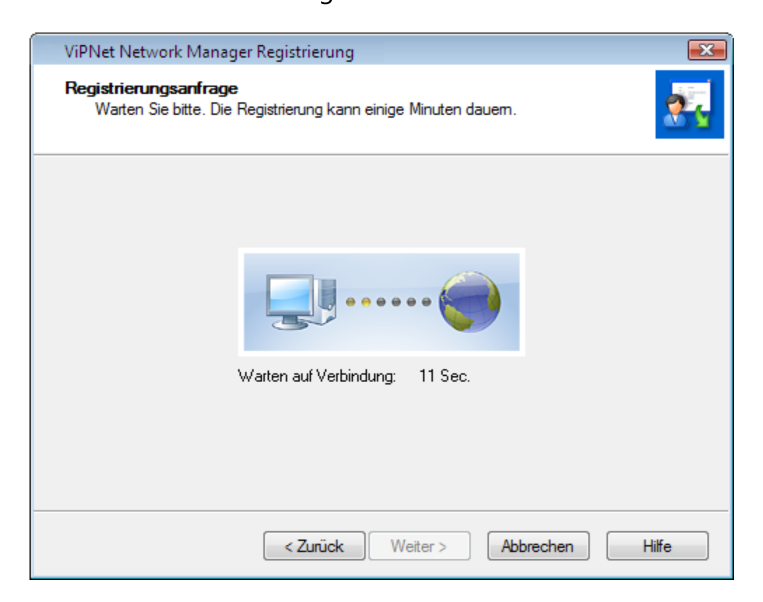


Abbildung 20. Aufbau einer Verbindung zum Server

Wenn innerhalb von 3 Minuten kein Verbindungsaufbau zum Server des Registrierungssystems von „Infotecs" erfolgt, wird eine entsprechende Meldung eingeblendet.

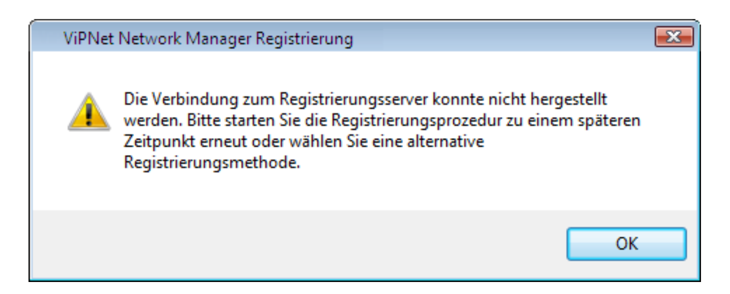


Abbildung 21. Fehler beim Verbindungsaufbau

Wenn die Verbindung zum Server des Registrierungssystems erfolgreich hergestellt wurde, aber die von Ihnen angegebenen Daten nicht korrekt sind, gibt das Programm eine diesbezügliche Meldung aus. Klicken Sie im Meldungsfenster auf **OK**. Sie kehren zum Assistentenfenster **Registrierungsdaten** zurück. Wenn die Registrierung verweigert wurde, wird wieder das Fenster **Registrierungsdaten** geöffnet. Überprüfen Sie die Richtigkeit der eingegebenen Seriennummer und versuchen Sie es erneut.

Wenn die Registrierung erfolgreich durchgeführt wurde, wird das Fenster **Die Registrierung von ViPNet Network Manager wurde erfolgreich abgeschlossen** eingeblendet. In diesem Fenster sind Empfehlungen für eine sichere Speicherung Ihrer Registrierungsdaten angegeben (s. Registrierungsdaten speichern auf S. 81).

7 Klicken Sie auf **Fertig**.

Registrierungsanfrage via E-Mail



Achtung! Für diese Registrierungsmöglichkeit ist ein Internet-Zugang und ein E-Mail Client erforderlich.

Wenn Sie die Registrierungsoption **Via E-Mail** gewählt haben, wird das Fenster **Registrierungsdaten** geöffnet. Im Fenster **Registrierungsdaten**:

1 Geben Sie alle Daten ein, wie im Abschnitt Registrierungsanfrage über das Internet (auf S. 74) beschrieben.

2 Klicken Sie auf **Weiter**. In Ihrem E-Mail-Programm wird eine neue Nachricht erstellt, die die von Ihnen angegebenen Registrierungsdaten enthält. Die E-Mail wird an den Empfänger reg@infotecs.biz adressiert.

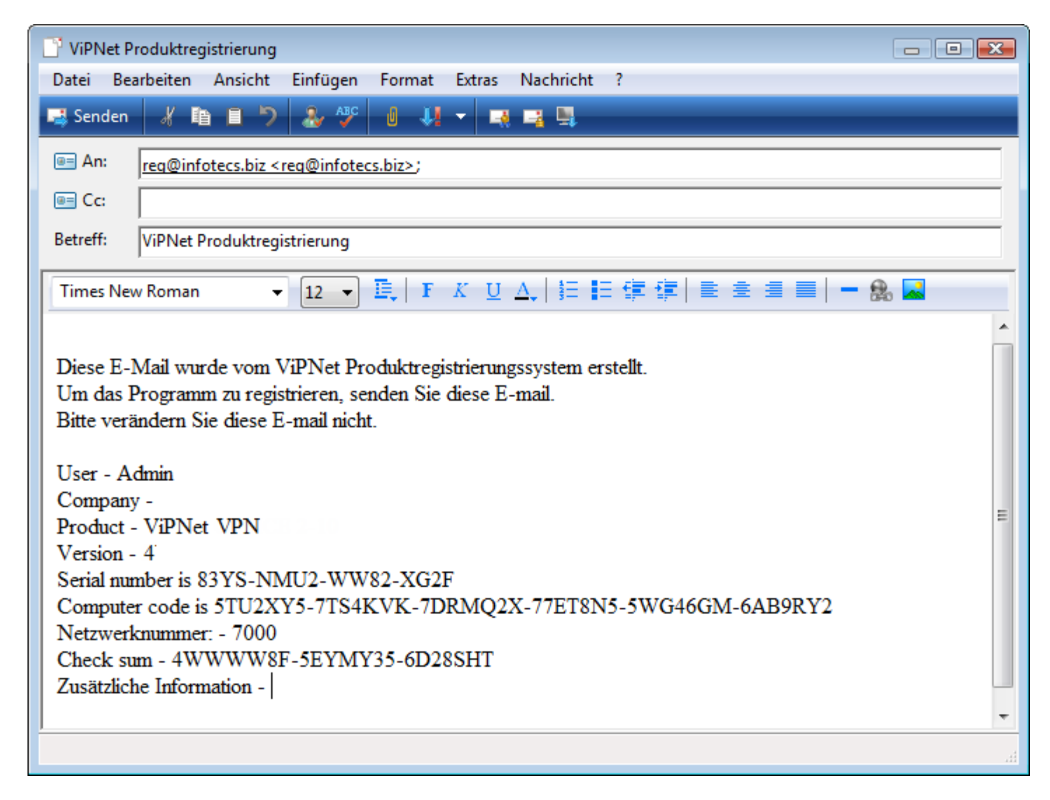


Abbildung 22. Registrierungscode via E-Mail anfordern



Achtung! Es wird empfohlen, die Nachricht mit den Registrierungsdaten nicht zu editieren.

3 Zum Abschließen der Registrierung senden Sie die E-Mail ab. Nach Überprüfung Ihrer Registrierungsdaten erhalten Sie den Registrierungscode via E-Mail.



Achtung! Wenn Sie innerhalb weniger Tage keine Rückmeldung von „Infotecs erhalten, versuchen Sie erneut, die Nachricht zu versenden. Dazu wiederholen Sie alle Schritte, die in diesem Abschnitt beschrieben sind. Wenn auch das nicht zu einer Registrierung von ViPNet Network Manager geführt hat, setzen Sie sich mit dem Kundendienst von „Infotecs in Verbindung.

4 Nach Erhalt der E-Mail mit dem Registrierungscode registrieren Sie Ihre Kopie von ViPNet Network Manager (s. ViPNet Network Manager registrieren auf S. 80).

Registrierungsanfrage per Telefon

Wenn Sie die Registrierungsoption **Per Telefon** gewählt haben, wird das Fenster **Registrierungsanforderung per Telefon** geöffnet.

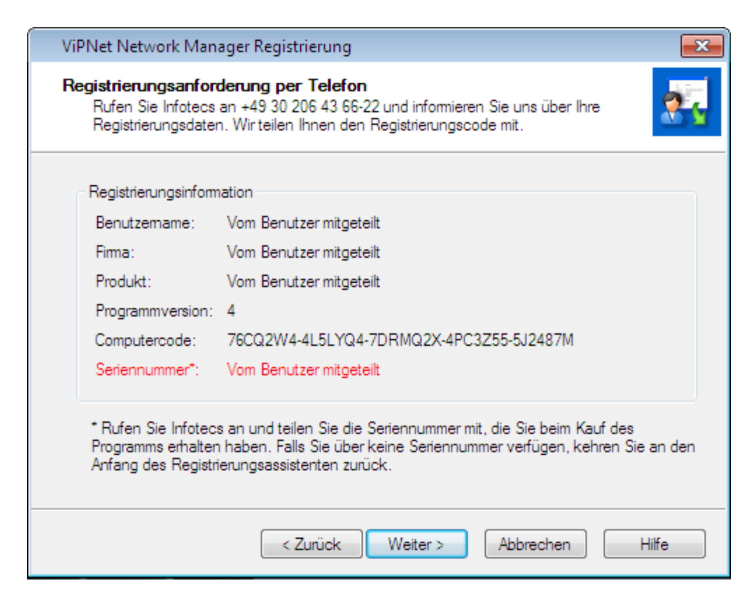


Abbildung 23. Registrierungscode per Telefon anfordern

In diesem Fenster sind alle Daten angegeben, die Sie einem Mitarbeiter von Infotecs bei der Registrierung mitteilen müssen.

1 Rufen Sie Infotecs GmbH unter der im oberen Fensterbereich angegebenen Nummer an und teilen Infotecs GmbH Ihre Registrierungsdaten mit. Als Antwort wird Ihnen der Registrierungscode mitgeteilt.

2 Nach Erhalt des Registrierungscodes klicken Sie auf **Weiter**. Es wird das Fenster **Registrieren** geöffnet.

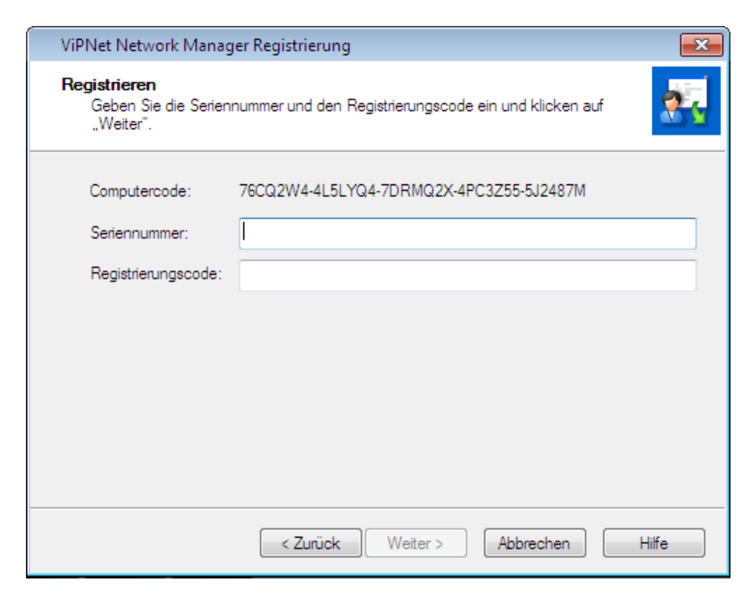


Abbildung 24. Registrierungscode eingeben

3 Geben Sie im Fenster **Registrieren** die Seriennummer und den Registrierungscode ein und klicken auf **Weiter**.



Hinweis. Wenn Sie die Seriennummer zu einem früheren Zeitpunkt bereits eingegeben haben, wird das Feld **Seriennummer** automatisch ausgefüllt.

Wenn die eingegebenen Daten korrekt sind, wird das Fenster **Die Registrierung von ViPNet Network Managerwurde erfolgreich abgeschlossen** eingeblendet. In diesem Fenster sind Empfehlungen für eine sichere Speicherung Ihrer Registrierungsdaten angegeben (s. Registrierungsdaten speichern auf S. 81).

4 Klicken Sie auf **Fertig**.

ViPNet Network Manager registrieren

Nachdem Sie von Infotecs GmbH den Registrierungscode erhalten haben, können Sie Ihre Kopie von ViPNet Network Manager registrieren. Dazu:

1 Starten Sie den Assistenten **ViPNet Network Manager Registrierung**.

2 Wählen Sie im ersten Fenster die Option **Registrieren** und klicken auf **Weiter**.

3 Geben Sie im Fenster **Seriennummer** die Seriennummer ein und klicken auf **Weiter**.

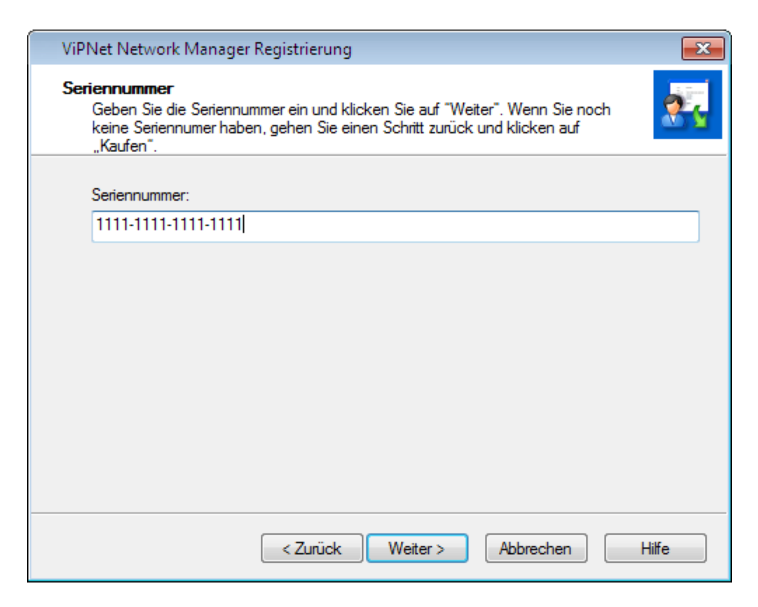


Abbildung 25. Seriennummer eingeben



Hinweis. Wenn Sie die Seriennummer zu einem früheren Zeitpunkt eingegeben haben, wird das Feld **Seriennummer** automatisch befüllt.

4 Geben Sie im Fenster **Registrierungscode** den Registrierungscode ein.

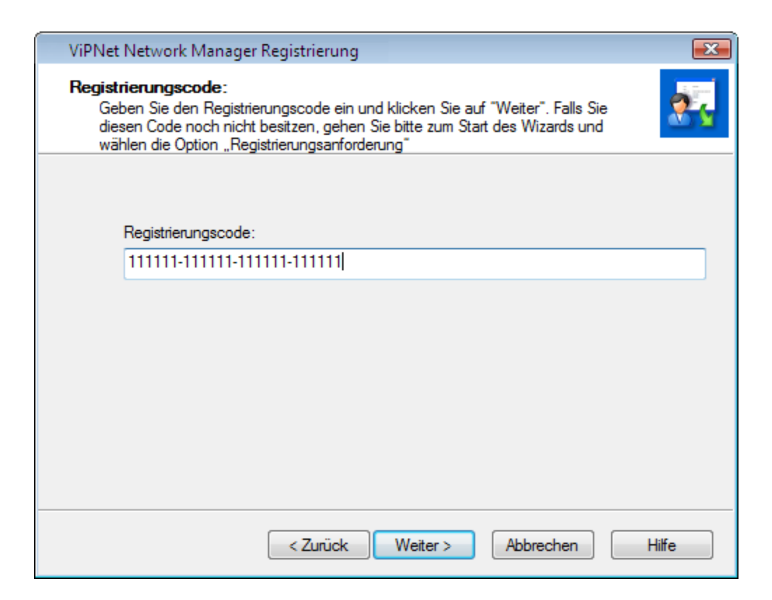


Abbildung 26. Registrierungscode eingeben

5 Klicken Sie auf **Weiter**. Wenn die von Ihnen eingegebenen Daten korrekt sind, wird das Fenster **Die Registrierung von ViPNet Network Manager wurde erfolgreich abgeschlossen** geöffnet.

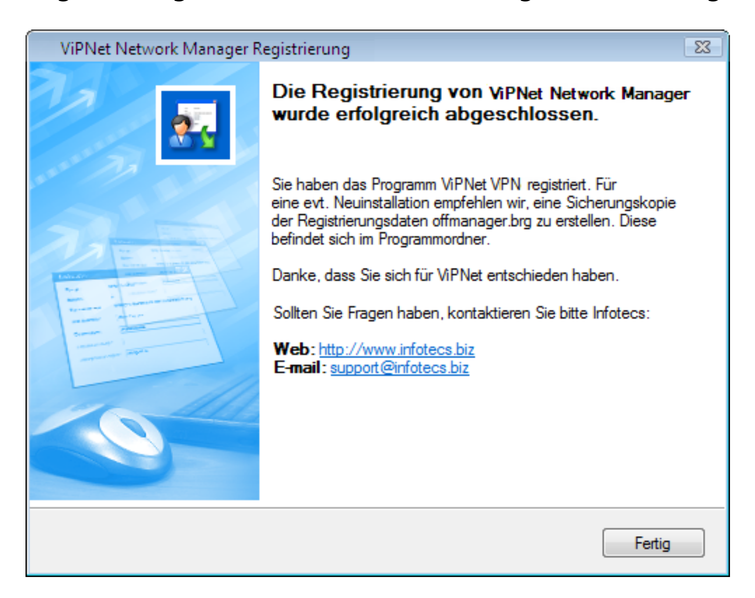


Abbildung 27. Registrierung von ViPNet Manager abgeschlossen

6 Klicken Sie auf **Fertig**.

7 Speichern Sie die Registrierungsdaten (s. Registrierungsdaten speichern auf S. 81), indem Sie die Datei *.brg, die sich im Installationsordner von ViPNet Network Manager befindet, an einen sicheren Ort kopieren.

Registrierungsdaten speichern

Nach Abschluss der Registrierung speichert das Programm die Registrierungsdaten in der Datei `offmanager.brg`, die im Ordner `C:\ProgramData\InfoTeCS\ViPNet Manager` neu angelegt wird.

Wir empfehlen, die Datei mit Registrierungsdaten an einen sicheren Ort zu kopieren, da diese Datei bei einer wiederholten Installation von ViPNet Network Manager (wenn Sie zum Beispiel das Programm in einem anderen Ordner neu installieren möchten oder wenn das Programm nach einer Formatierung der Festplatte erneut installiert werden soll) von Nutzen sein kann. In diesem Fall wird die gesicherte Datei `offmanager.brg` in den `Ordner C:\ProgramData\InfoTeCS\ViPNet Manager` kopiert. Nach einem Neustart des Computers wird dann das neu installierte Programm automatisch registriert (wenn die Registrierungsdaten korrekt sind, und sich die Konfiguration des Computers nicht geändert hat).

Wenn sich die Konfiguration Ihres Computers geändert hat

Eine Erneuerung der Konfiguration des Computers, auf dem ViPNet Network Manager installiert ist, kann Auswirkungen auf die Funktionsweise des Programms haben. Wenn die Änderungen signifikant sind (es wurde zum Beispiel ein Großteil der Komponenten ersetzt), muss Ihre Kopie von ViPNet Network Manager neu registriert werden (s. Registrierungscode anfordern auf S. 74). Wenn die Änderungen in der Konfiguration des Computers unwesentlich sind, muss ViPNet Network Manager nicht neu registriert werden.

Beim ersten Start von ViPNet Network Manager nach einer unwesentlichen Änderung der Computerkonfiguration wird vom Programm die Meldung ausgegeben, dass aufgrund einer Änderung der Computerkonfiguration eine neue `*.brg` Datei erzeugt wurde. Das bedeutet, dass die ursprüngliche Registrierungsdatei veraltet ist, und Sie die Datei nicht mehr für eine erneute Registrierung des Programms nach einer Neuinstallation verwenden können.

Kopieren Sie die neue Datei `*.brg` an einen sicheren Ort. Wenn Sie ViPNet Network Manager neu installieren, kopieren Sie diese Datei in den Ordner `C:\ProgramData\InfoTeCS\ViPNet Manager` und das Programm wird automatisch registriert.



Arbeit beginnen. Erstellen der ViPNet Struktur

Erstmaliges Starten von ViPNet Network Manager

Zum Starten von ViPNet Network Manager:

1 Führen Sie einen der folgenden Schritte aus:

- Verwenden Sie das Betriebssystem Windows 7 oder eine frühere Version, wählen Sie im Menü **Start** den Eintrag **Alle Programme** > **ViPNet** > **ViPNet Network Manager** > **ViPNet Network Manager**.
- Verwenden Sie das Betriebssystem Windows 8 oder eine spätere Version, öffnen Sie die Apps-Liste auf der Startseite und wählen den Eintrag **ViPNet** > **ViPNet Network Manager**.

2 Es wird das Fenster zur Erstellung des Administratorpassworts von ViPNet Network Manager geöffnet. Geben Sie das Passwort ein, das für die Anmeldung in ViPNet Network Manager verwendet werden soll. In der Liste **Passworttyp** kann eine der Optionen **Benutzerdefiniertes** oder **Zufälliges** ausgewählt werden. Nachdem Sie ein Passwort definiert haben, klicken Sie auf **OK**.



Abbildung 28. Administratorpasswort für ViPNet Network Manager erstellen

3 Führen Sie die Schritte aus, die im eingeblendeten Fenster Digitales Roulette aufgeführt sind. Wenn das digitale Roulette in der laufenden Sitzung bereits gestartet wurde, wird dieses Fenster nicht angezeigt.

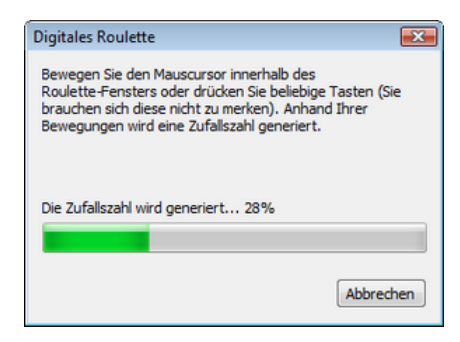


Abbildung 29. Digitales Roulette

Es wird der **ViPNet Netzwerkaufbau Assistent** geöffnet, mit dessen Hilfe Sie die Basisstruktur des Netzwerks erstellen können (s. Automatische Generierung der ViPNet Netzwerkstruktur auf S. 86). Wenn Sie die Netzwerkstruktur später definieren möchten, klicken Sie im Assistentenfenster auf **Schließen**.

Erstellen des ViPNet Netzwerks

Automatische Generierung der ViPNet Netzwerkstruktur

Beim ersten Start von ViPNet Network Manager wird der ViPNet Netzwerkaufbau Assistent gestartet. Mit seiner Hilfe kann die Struktur des ViPNet Netzwerks angelegt, Schlüsseldistributionen für die Netzwerkknoten erstellt und Passwörter für alle ViPNet Benutzer erzeugt werden.



Hinweis. Der **ViPNet Netzwerkaufbau** Assistent kann aus dem Hauptfenster von ViPNet Network Manager gestartet werden. Wählen Sie dazu im Menü **Netzwerk** die Option **Erstellen**. Dabei wird die bestehende Netzwerkstruktur gelöscht.

Um die Struktur eines ViPNet Netzwerks zu erstellen:

1 Klicken Sie auf der ersten Seite des **ViPNet Netzwerkaufbau**-Assistenten auf die Schaltfläche **Weiter**.

2 Wählen sie auf der Seite **Standort des Manager-Arbeitsplatzes** den Typ des Netzwerkknotens, auf dem Sie den Manager-Arbeitsplatz einrichten möchten.

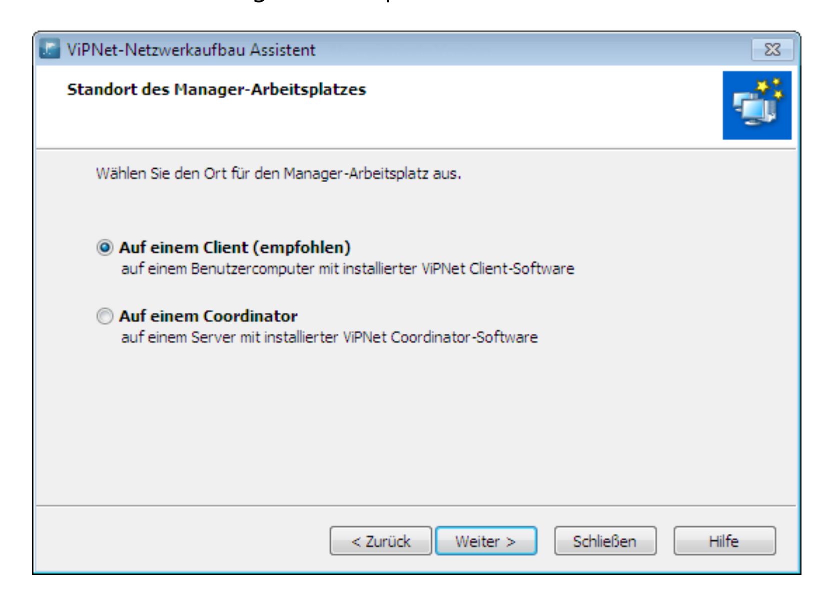


Abbildung 30. Standort der Manager-Arbeitsplatzes

3 Klicken Sie auf der Seite Standort des Manager-Arbeitsplatzes auf **Weiter**. Es wird die Seite **Automatische Generierung der ViPNet Struktur** geöffnet.

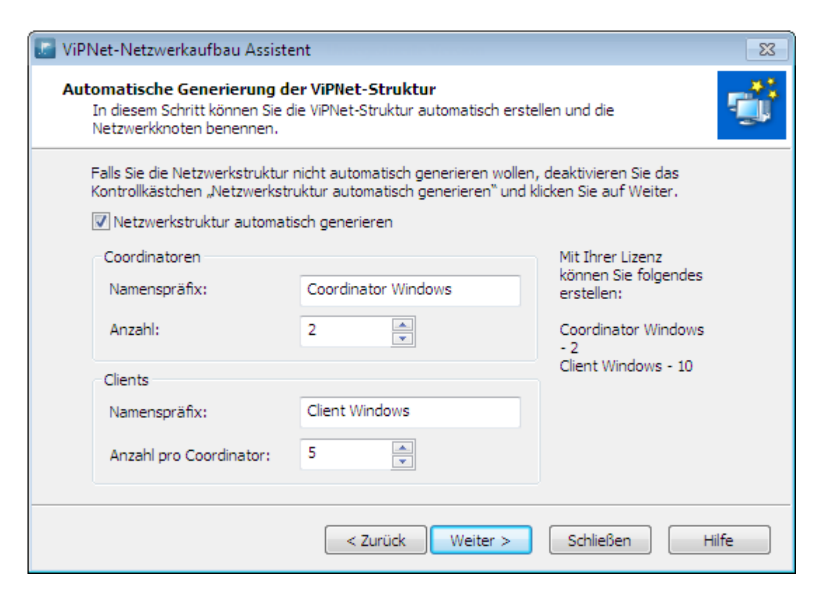


Abbildung 31. Automatische Generierung der ViPNet-Netzwerkstruktur

4 Wenn die Struktur manuell erstellt werden soll:

- Deaktivieren Sie die Option **Netzwerkstruktur automatisch generieren**.
- Klicken Sie zum Fortsetzen auf **Weiter**. Es wird das Fenster **Netzwerkstruktur generieren** geöffnet.
- Erstellen Sie die gewünschte Netzwerkstruktur (s. Ändern der ViPNet Netzwerkstruktur auf S. 89).

5 Lassen Sie das Kontrollkästchen **Netzwerkstruktur automatisch generieren** aktiv, wenn die Netzwerkstruktur automatisch generiert werden soll.

Standardmäßig wird die maximal zulässige, von der Lizenz erlaubte Anzahl an Coordinatoren ViPNet Coordinator für Windows und Clients ViPNet Client für Windows angelegt.



Achtung! Beim automatischen Erstellen der Netzwerkstruktur können ausschließlich Clients vom Typ ViPNet Client Windows und Coordinatoren vom Typ ViPNet Coordinator Windows angelegt werden. Clients und Coordinatoren anderer Typen können manuell auf der Seite **Ändern der ViPNet Struktur** zum Netzwerk hinzugefügt werden.

---

6 Klicken Sie auf **Weiter**, um zur Seite **Automatische Verbindungsgenerierung** zu wechseln.

Generieren von Verbindungen zwischen ViPNet Netzwerkknoten



Hinweis. Die Seite **Automatische Verbindungsgenerierung** wird nur dann angezeigt, wenn die beim vorhergehenden Schritt angegebene Anzahl an Clients größer Null ist.

Führen Sie auf der Seite **Automatische Verbindungsgenerierung** die folgenden Schritte durch:

1 Wählen Sie mit Hilfe der Optionsfelder die benötigte Art der Verbindung:

- **Alle Netzwerkknoten miteinander verbinden** – Standardoption. Alle Netzwerkknoten werden miteinander verbunden.
- **Alle Clients eines Coordinators miteinander verbinden** – alle Clients, die zum selben Coordinator gehören werden sowohl miteinander als auch mit dem eigenen Coordinator verbunden. Zusätzlich werden alle Coordinatoren untereinander verbunden.
- **Jeden Client nur mit seinem Coordinator verbinden** – jeder Client wird nur mit seinem Coordinator verbunden. Dabei werden alle Coordinatoren untereinander verbunden.

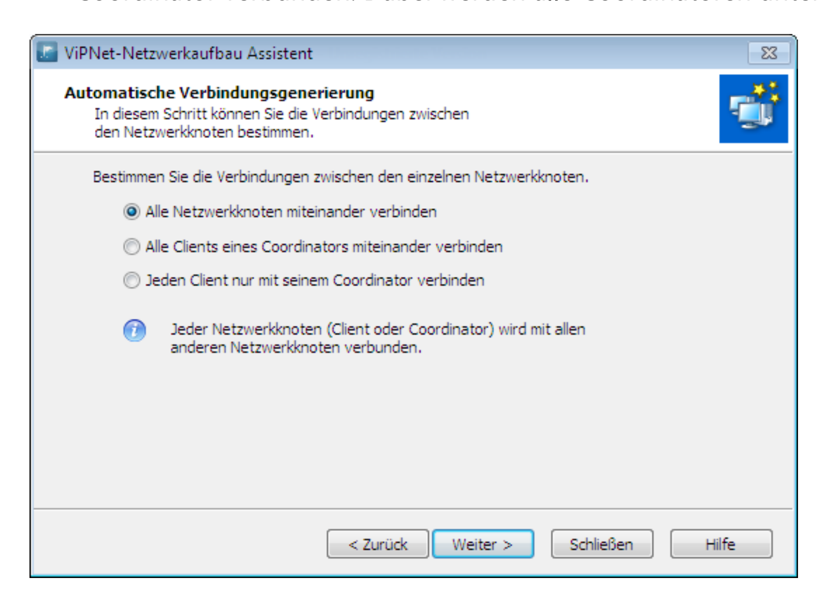


Abbildung 32. Seite zur automatischen Verbindungsgenerierung

2 Klicken Sie auf **Weiter**. Die automatische Generierung von Verbindungen zwischen den Netzwerkknoten wird gestartet. Dieser Vorgang kann einige Zeit in Anspruch nehmen, besonders dann, wenn die Anzahl der Netzwerkknoten größer als 100 ist.

Wenn die Generierung der Verbindungen zwischen den Netzwerkknoten abgeschlossen ist, wird die Seite **Ändern der ViPNet Struktur** geöffnet.

Ändern der ViPNet Netzwerkstruktur

Auf der Seite **Ändern der ViPNet Struktur** können Sie die automatisch erstellte Netzwerkstruktur bearbeiten oder eine eigene Struktur neu erstellen (entsprechend der vorhandenen Lizenz). Die Lizenzinformationen werden im rechten Teil des Fensters **Ändern der ViPNet Struktur** angezeigt. Wenn die Anzahl von Netzwerkknoten den maximalen in der Lizenz bestimmten Wert erreicht, wird die folgende Mitteilung ausgegeben: **Maximale Größe der Netzwerkstruktur ist erreicht**.

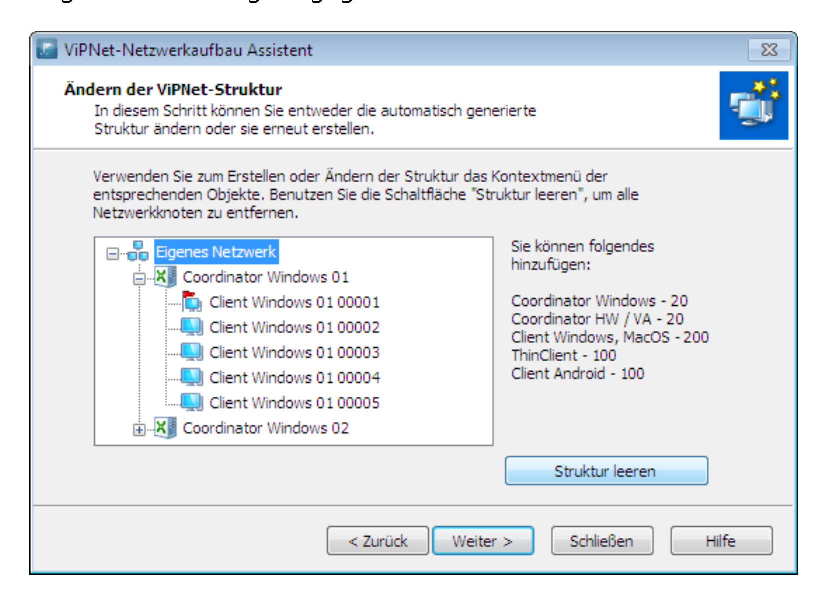


Abbildung 33. Seite zum Ändern der ViPNet-Netzwerkstruktur

In der automatisch erstellten Netzwerkstruktur setzen sich die Namen der Coordinatoren und Clients aus einem vorgegebenen Präfix (s. Automatische Generierung der ViPNet Netzwerkstruktur auf S. 86) und der laufenden Nummer des Knotens zusammen.

In Abhängigkeit vom gewählten Standorttyp wird der erste Client des ersten Coordinators automatisch als Manager-Arbeitsplatz festgelegt (auf dem Knoten mit dem Manager-Arbeitsplatz wird das Programm ViPNet Network Manager installiert) und mit dem Symbol oder gekennzeichnet.

Wenn nötig, gehen Sie wie folgt vor, um die Netzwerkstruktur zu ändern:

- Klicken Sie zum Hinzufügen eines Coordinators mit der rechten Maustaste auf das Element **Eigenes Netzwerk** und wählen im Kontextmenü den erforderlichen Typ des neuen Coordinators aus.
- Klicken Sie zum Hinzufügen eines Clients mit der rechten Maustaste auf einen der Coordinatoren und wählen im Kontextmenü den Typ des neuen Clients aus.
- Klicken Sie zum Löschen des Netzwerkknotens mit der rechten Maustaste auf diesen Netzwerkknoten und wählen den Eintrag **Löschen**.
- Klicken Sie zum Umbenennen des Netzwerkknotens mit der rechten Maustaste auf diesen Netzwerkknoten und wählen den Eintrag **Umbenennen**.



Hinweis. Die Namen der Netzwerkknoten sollten innerhalb eines ViPNet Netzwerks eindeutig sein. Wenn der gewählte Name bereits existiert, schlägt das Programm einen anderen Namen vor.

- Um einen Netzwerkknoten als Manager-Arbeitsplatz zu bestimmen (auf dem Netzwerkknoten muss das Programm ViPNet Network Manager installiert sein), klicken Sie mit der rechten Maustaste auf diesen Netzwerkknoten und wählen Sie im Kontextmenü die Option **Als Manager-Arbeitsplatz festlegen**.
- Damit die Verwendung von ViPNet StateWatcher oder ViPNet Policy Manager auf dem gewählten Client erlaubt wird, klicken Sie mit der rechten Maustaste auf den Client und wählen im Kontextmenü den Befehl **StateWatcher zulassen** oder **Policy Manager zulassen**.
- Zum Verschieben eines Clients von einem Coordinator auf einen anderen klicken Sie auf den Client und ziehen ihn auf den neuen Coordinator.

Zum Speichern der erstellten ViPNet Netzwerkstruktur klicken Sie auf **Weiter**. Es wird die Seite **Bearbeiten der Verbindungen** geöffnet.

Bearbeiten der Verbindungen

Auf der Seite **Bearbeitung der Verbindungen** können die Verbindungen zwischen den einzelnen Netzwerkknoten im ViPNet Netzwerk geändert werden.

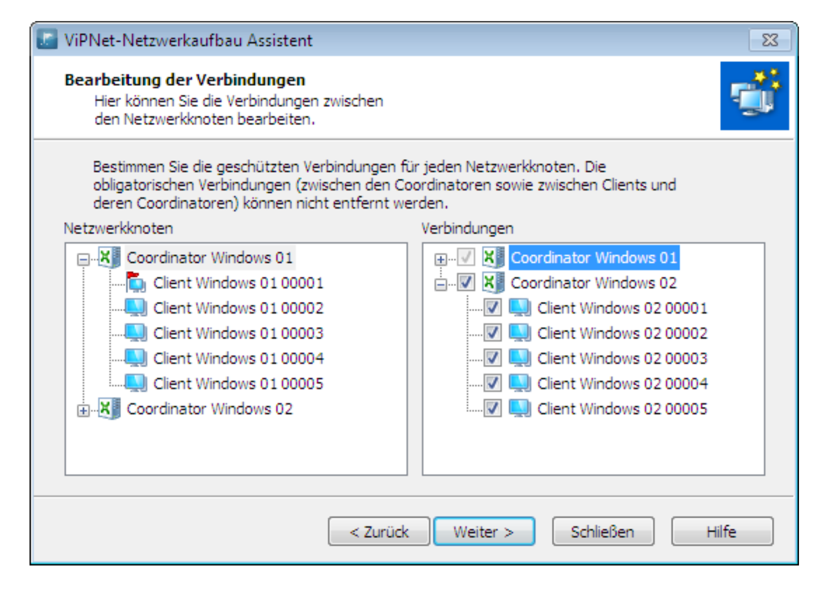


Abbildung 34. Bearbeitung der Verbindungen zwischen den Netzwerkknoten

Damit zwei Netzwerkknoten nicht miteinander kommunizieren können, darf zwischen ihnen keine Verbindung bestehen. Dann sind diese Netzwerkknoten füreinander nicht sichtbar und können die Programme Business Mail, Chat und andere ViPNet Anwendungen nicht dazu verwenden, miteinander zu kommunizieren. Dennoch gehören diese Netzwerkknoten weiterhin zum ViPNet Netzwerk, ihr IP-Traffic bleibt geschützt.

Wenn alle Verbindungen eines Netzwerkknotens (außer den obligatorischen Verbindungen) gelöscht werden, wird dieser Netzwerkknoten vollständig vom restlichen ViPNet Netzwerk isoliert.

Um Verbindungen des beliebigen Netzwerkknotens zu ändern, führen Sie folgende Aktionen durch:

1 Klicken Sie in der Panel **Netzwerkknoten** auf den Netzwerkknoten.

2 Aktivieren oder deaktivieren Sie einen Kontrollkästchen neben Netzwerkknoten, zu dem eine Verbindung aufgebaut oder gelöscht werden soll.



Hinweis. Obligatorische Verbindungen (Verbindungen zwischen Coordinatoren und Verbindungen zwischen Netzwerkknoten und Coordinatoren, auf denen diese registriert sind) dürfen nicht gelöscht werden.

Wenn die Bearbeitung von Verbindungen abgeschlossen ist, klicken Sie auf **Weiter**. Es wird die Seite **Konfigurieren des Zugangs auf den Coordinator** geöffnet.

Konfiguration des Zugangs zum Coordinator

Auf der Seite **Konfiguration des Zugriffs auf den Coordinator** wird die Art der Verbindung des Coordinators zum Internet festgelegt. Abhängig von der Auswahl können weitere Einstellungen für den Coordinatorzugang konfiguriert werden.



Hinweis. Mit Hilfe des ViPNet Netzwerkaufbauassistenten kann ausschließlich der Zugang zum Coordinator, auf dem der Manager-Arbeitsplatz registriert ist, konfiguriert werden. Wenn die Lizenz die Erstellung mehrerer Coordinatoren erlaubt, kann der Zugang zu anderen Coordinatoren im Programm ViPNet Network Manager konfiguriert werden.

Konfiguration des Zugangs auf den Coordinator, der unmittelbar mit dem Internet verbunden ist

Wenn der Coordinator unmittelbar mit dem Internet verbunden ist:

1 Wählen Sie in der Liste **Verbindung ins Internet** den Eintrag **Direkte Verbindung**.

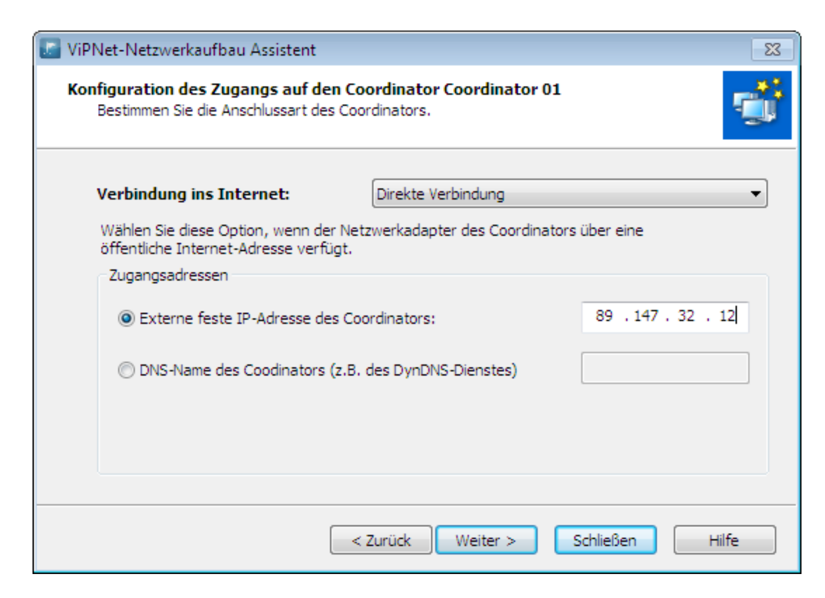


Abbildung 35. Coordinator verfügt über direkte Verbindung zum Internet

2 Wählen Sie in der Gruppe **Zugangsadressen** einen der folgenden Zugangsparameter:

- Wenn der Coordinator über eine statische IP-Adresse verfügt, wählen Sie die Option **Externe feste IP-Adresse des Coordinators** und geben die öffentliche IP-Adresse des Coordinators im Feld rechts davon ein. Andere Netzwerkknoten des externen Netzwerks können den Coordinator über diese IP-Adresse erreichen.
- Wenn der Coordinator über eine dynamische IP-Adresse verfügt, wählen Sie die Option **DNS-Name des Coordinators (z.B. des DynDNS-Dienstes)** und geben den DNS-Namen des Coordinators im Feld rechts davon ein.



Hinweis. Wenn Sie den DNS-Namen des Coordinators verwenden, stellen Sie sicher, dass der Coordinator unter diesem Namen auf dem DNS-Server registriert ist.

3 Klicken Sie auf **Weiter**. Es wird das Fenster **Eigenschaften des Zufallszahlengenerators** geöffnet.

Konfiguration des Zugang zum Coordinator, der über eine Firewall mit dem Internet verbunden ist

Wenn der Coordinator über eine Firewall oder einen DSL-Router, auf dem statische NAT-Regeln definiert werden können, mit dem Internet verbunden ist:

1 Wählen Sie in der Liste **Verbindung ins Internet** den Eintrag **Verbindung über eine Firewall**.

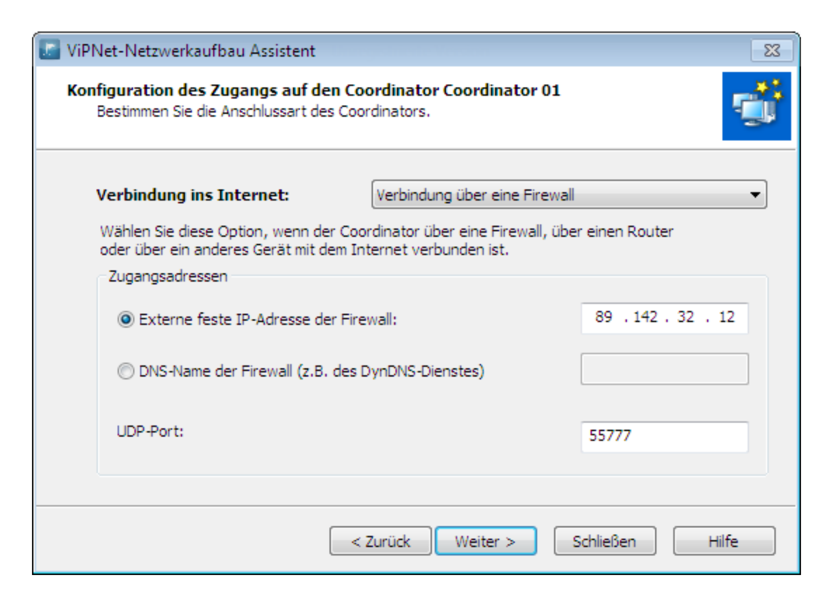


Abbildung 36. Coordinator ist über eine Firewall mit dem Internet verbunden

2 Wählen Sie in der Gruppe **Zugangsadressen** einen der folgenden Zugangsparameter:

- Wenn die Firewall, über die der Coordinator mit dem Internet verbunden ist, über eine statische IP-Adresse verfügt, wählen Sie die Option **Externe feste IP-Adresse der Firewall** und geben die IP-Adresse der Firewall ein.
- Wenn die Firewall über eine dynamisch vergebene IP-Adresse verfügt, wählen Sie die Option **DNS-Name der Firewall (z.B. des DynDNS-Dienstes)** und geben den DNS-Namen der Firewall ein.

3 Geben Sie im Feld **UDP-Port** die Portnummer ein, die in den Einstellungen der Firewall zum Sicherstellen des Zugangs externer Knoten zum Coordinator festgelegt ist. Standardmäßig ist Port 55777 definiert.

4 Klicken Sie auf **Weiter**. Es wird die Seite **Eigenschaften des Zufallsgenerators** geöffnet.

Konfiguration des Zugang auf den Coordinator im Hauptfenster von ViPNet Network Manager

Es besteht die Möglichkeit, die Konfiguration des Zugangs zum Coordinator zu einem späteren Zeitpunkt im Programm ViPNet Network Manager durchzuführen. Wählen Sie dazu in der Liste **Verbindung ins Internet** den Eintrag **Später im ViPNet Network Manager konfigurieren**.

Klicken Sie auf **Weiter**. Es wird das Fenster **Eigenschaften des Zufallsgenerators** geöffnet.

Konfiguration der Eigenschaften zufälliger Passwörter

Auf der Seite **Eigenschaften des Zufallsgenerators** kann das Verfahren zur Erzeugung zufälliger Passwörter für die Netzwerkbenutzer geändert werden.

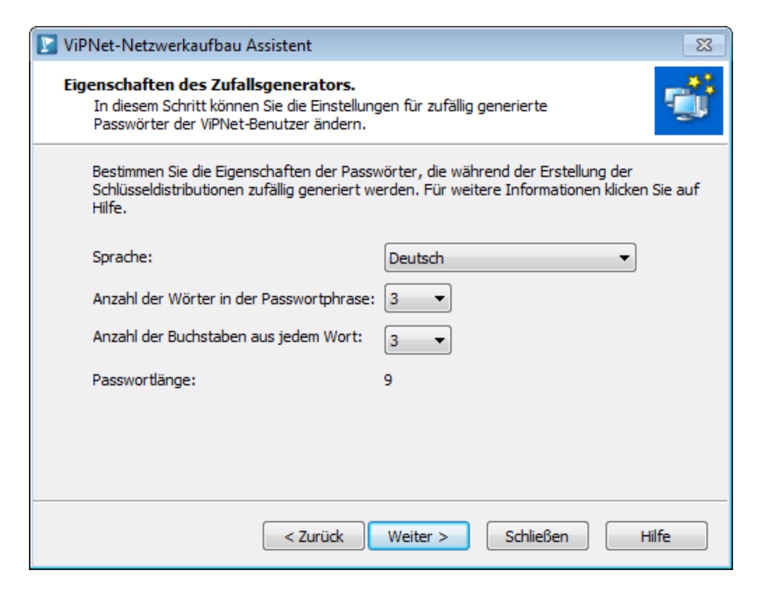


Abbildung 37. Eigenschaften zufälliger Passwörter

Jeder Netzwerkknoten (Client oder Coordinator) verfügt über ein eigenes Benutzerpasswort. Das Benutzerpasswort wird mit Hilfe der ersten N Buchstaben jedes Wortes einer zufällig generierten Passwortphrase erstellt.

Ausführliche Beschreibung der Eigenschaften zufälliger Passwörter s. Abschnitt Konfiguration der Eigenschaften der Benutzerpasswörter (auf S. 139).

Klicken Sie auf **Weiter**. Es wird die Seite **Abschließen des ViPNet Netzwerkaufbau-Assistenten** geöffnet.

Erstellung des ViPNet Netzwerkes abschließen

Gehen Sie auf der Seite **Abschließen des ViPNet Netzwerkaufbau-Assistenten** wie folgt vor:

1 Wenn die Erstellung von Schlüsseldistributionen zu diesem Zeitpunkt nicht erforderlich ist, deaktivieren Sie das Kontrollkästchen **Die Schlüsseldistributionen werden nach dem Beenden des Assistenten erstellt**.



Achtung! Vor dem erstmaligen Erstellen der Schlüsseldistributionen für alle Netzwerkknoten sollte für jeden Coordinator zumindest eine Zugangsadresse definiert werden. Anderenfalls kann es zu Problemen mit der Funktionsfähigkeit bestimmter Typen von Clients kommen. Deswegen empfehlen wir, die Schlüsseldistributionen der Netzwerkknoten (s. Erstellung von Schlüsseldistributionen, nachdem die Netzwerkstruktur mit Hilfe des Assistenten generiert wurde auf S. 95) später mit Hilfe des Programms ViPNet Network Manager zu erstellen. Dadurch kann außerdem eine gesonderte manuelle Konfiguration jedes einzelnen Netzwerkknotens vermieden werden.

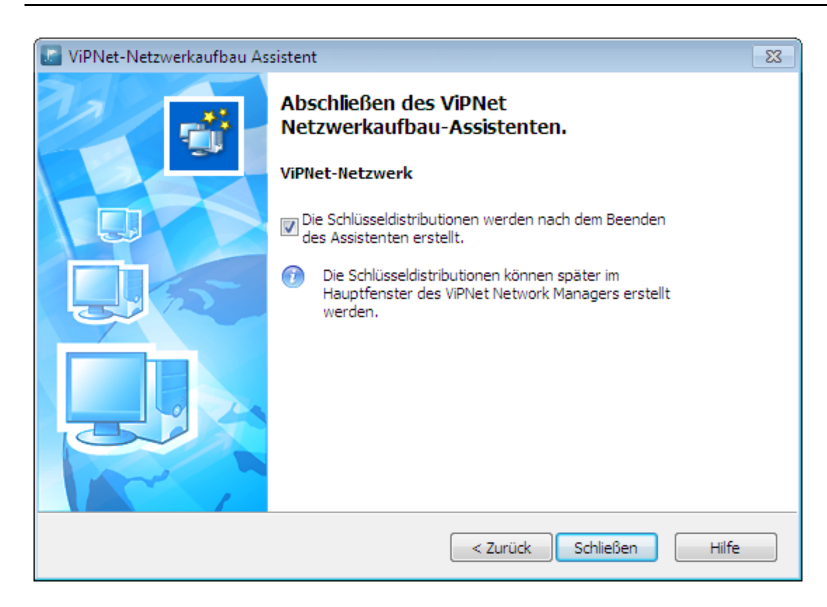


Abbildung 38. Abschließen des ViPNet-Netzwerkaufbau-Assistenten

2 Klicken Sie auf **Schließen**, um die Arbeit des Assistenten abzuschließen.

Erstellung von Schlüsseldistributionen, nachdem die Netzwerkstruktur mit Hilfe des Assistenten generiert wurde

Wenn auf der Seite **Abschließen des ViPNet Netzwerkaufbau-Assistenten** (s. Abbildung 38 auf S. 95) das Kontrollkästchen **Die Schlüsseldistributionen werden nach dem Beenden des Assistenten erstellt** aktiviert wurde, wird nun mit der Erstellung der Schlüsseldistributionen für die Netzwerkknoten begonnen:

1 Es wird das Fenster **Ordner auswählen** geöffnet. Geben Sie in diesem Fenster den Ordner an, in welchem die Netzwerkknotenschlüssel gespeichert werden sollen.

2 Wenn die Erstellung der Schlüssel abgeschlossen ist, wird im Explorer-Fenster von Windows der Ordner angezeigt, in welchem die zuvor erstellten Netzwerkknotenschlüssel sowie die Benutzer- und Administratorpasswörter von ViPNet gespeichert wurden.

Die Dateien der Schlüsseldistributionen besitzen die Erweiterung `.dst` und werden in Ordnern abgelegt, deren Namen den Netzwerkknotennamen entsprechen. Benutzerpasswörter werden in der Datei `ViPNet.txt` in Form einer Liste abgelegt. Das gemeinsame Administratorpasswort für alle ViPNet Netzwerkknoten wird im Bereich **Eigenes Netzwerk** in der Registerkarte **Passwörter** angezeigt.

3 Kopieren Sie die Schlüssel und die Benutzerkennwörter auf einen Wechseldatenträger (z. B. CD oder USB-Stick). Diese Kopien der Schlüsseldistributionen können bei der Installation von ViPNet Software auf Coordinatoren und Clients verwendet werden. Stellen Sie sicher, dass der externe Datenträger mit den Schlüsseldistributionen auf allen Computern innerhalb des Netzwerks verwendet werden kann.

Starten und Beenden von ViPNet Network Manager

Zum Starten von ViPNet Network Manager:

1 Führen Sie einen der folgenden Schritte durch:

   - Verwenden Sie das Betriebssystem Windows 7 oder eine frühere Version, wählen Sie im Menü **Start** den Eintrag **Alle Programme** > **ViPNet** > **ViPNet Network Manager** > **ViPNet Network Manager**.
   - Verwenden Sie das Betriebssystem Windows 8 oder eine spätere Version, öffnen Sie die Apps-Liste auf der Startseite und wählen den Eintrag **ViPNet** > **ViPNet Network Manager**.

2 Das Passworteingabefenster wird geöffnet. Geben Sie das Manager-Passwort und klicken auf **OK**.

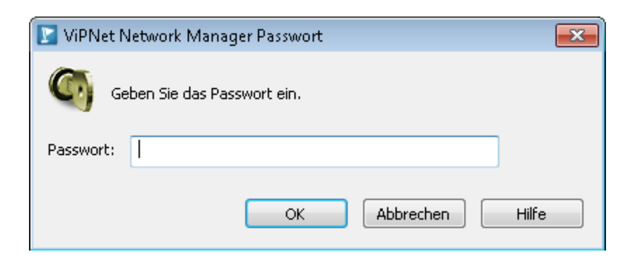


Abbildung 39. ViPNet Network Manager-Passwort eingeben

Führen Sie einen der folgenden Schritte durch, um ViPNet Network Manager zu schließen:

- Wählen Sie im Menü **Netzwerk** den Eintrag **Beenden**.
- Drücken Sie die Tastenkombination **Alt+F4**.
- Klicken Sie auf die Schaltfläche **Schließen** im oberen rechten Bereich des ViPNet Network Manager-Hauptfenster.

Benutzeroberfläche von ViPNet Network Manager

Das ViPNet Network Manager Hauptfenster ist auf der folgenden Abbildung dargestellt:

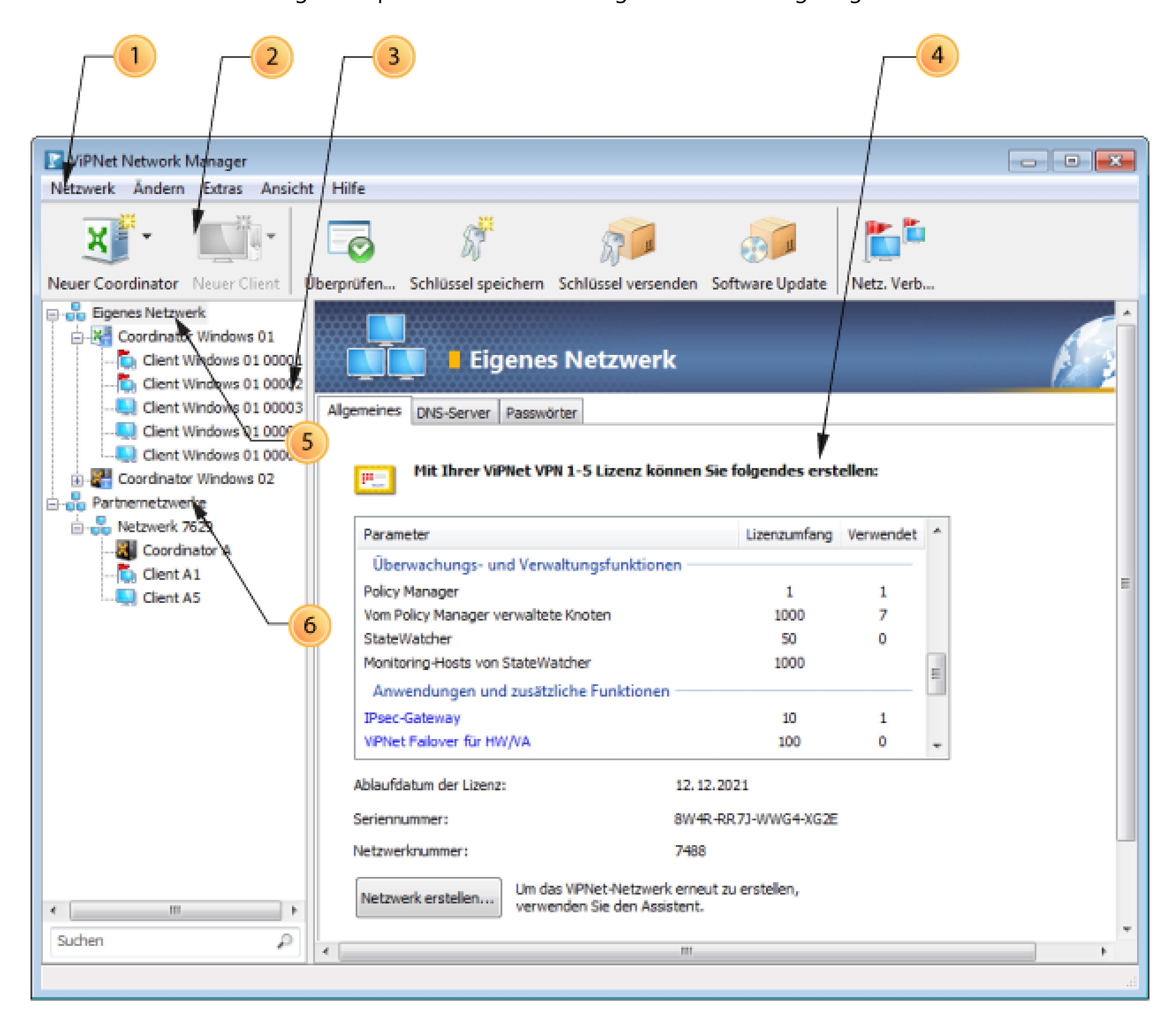


Abbildung 40. Hauptfenster des Programms ViPNet Network Manager

Mit Zahlen sind folgende Komponenten gekennzeichnet:

1 Hauptmenü des Programms.

2 Symbolleiste. Zum Hinzufügen oder Entfernen von Buttons, wählen Sie unter **Ansicht** die Option **Symbolleiste konfigurieren**.

3 Navigationsleiste mit der Struktur des Netzwerks in Form eines Ordnerbaumes.

4 Panel-Ansicht, die Registerkarten mit den Eigenschaften des in der Navigationsleiste gewählten Elements enthält.

5 **Eigenes Netzwerk**. Enthält alle Coordinatoren und Clients des eigenen ViPNet Netzwerks.

6 **Partnernetzwerke**. Wird nur angezeigt, wenn Partnernetzwerk-Verbindungen zu anderen ViPNet Netzwerken aufgebaut wurde (s. Partnernetzwerk-Verbindungen auf S. 165). Enthält die Auflistung aller Netzwerkknoten des Partnernetzwerks, zu denen eine Verbindung aufgebaut werden kann.

Ordner „Eigenes Netzwerk"

Wenn in der Navigationsleiste der Ordner **Eigenes Netzwerk** ausgewählt wird (s. Abbildung 40 auf S. 98), werden folgende Informationen über das ViPNet Netzwerk angezeigt:

Tabelle 7. Eigenschaften eigenes Netzwerks

Registerkarte	Beschreibung
Allgemeines	In der Registerkarte **Allgemeines** können folgende Informationen abgerufen werden: • Lizenzeinschränkung für die Einrichtung von Netzwerkknoten unterschiedlicher Typen, für die Anzahl getunnelter Verbindungen und für die Benutzung der zusätzlichen Komponenten ViPNet StateWatcher, ViPNet Policy Manager, ViPNet SafeDisk-V, ViPNet Business Mail. • Ablaufdatum der verwendeten Lizenz. • Listen von Knotentypen, die in der Lizenz erlaubt sind. • Knotenlisten, auf denen die Funktion des IPsec-Gateways verwendet wird. • Anzahl verwendeter Lizenzen für die Einrichtung von Netzwerkknoten unterschiedlicher Typen, für getunnelte Verbindungen und für die Benutzung der zusätzlichen Komponenten. • Netzwerknummer und Seriennummer des Programms (falls das Programm registriert ist). Die Lizenzeinschränkungen für zusätzliche ViPNet Komponenten können in der Registerkarte **Allgemeines** verteilt werden (s. Verwendung zusätzlicher ViPNet Komponenten auf S. 123).
DNS-Server	In dieser Registerkarte kann die Liste der geschützten DNS-Server Ihres Netzwerkes festgelegt werden (s. Liste der DNS-Server auf S. 125).
Passwörter	In dieser Registerkarte kann das Administratorpasswort des Netzwerkknotens abgerufen werden (s. Netzwerkknotenadministrator-Passwort auf S. 371).

Wenn in der Navigationsleiste ein Netzwerkknoten aus dem eigenen ViPNet Netzwerk angeklickt wird, werden in der Panel-Ansicht die Eigenschaften des Netzwerkknotens auf mehreren Registerkarten angezeigt:

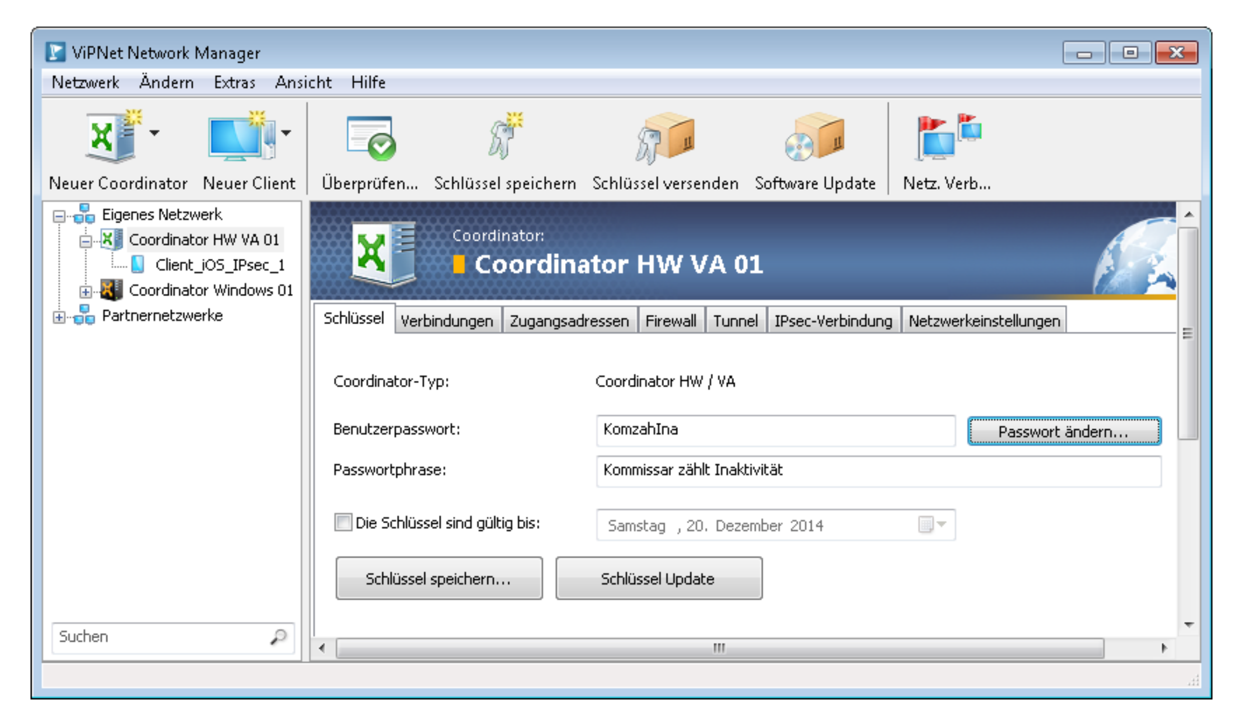


Abbildung 41. Eigenschaften eines Netzwerkknotens

Tabelle 8. Registerkarten in der Panel-Ansicht

Registerkarte	Beschreibung
Schlüssel	In dieser Registerkarte werden das Benutzerpasswort des Netzwerkknotens und Daten über die Schlüsseldistribution angezeigt.
Verbindungen	In dieser Registerkarte werden die Verbindungen des Netzwerkknotens angezeigt. Kommunikation ist nur dann möglich, wenn die Knoten mit einander verbunden sind (s. Ändern der Verbindungen zwischen den Netzwerkknoten auf S. 135).
Zugangsadressen (nur für Coordinator)	In dieser Registerkarte können die IP-Adressen oder DNS-Namen des gewählten Coordinators, sowie IP-Adressen oder DNS-Namen der Firewall dieses Coordinators (s. Zugriffs-IP-Adressen der Coordinatoren auf S. 109).
Firewall (nur für Coordinator)	In dieser Registerkarte kann die Konfiguration der Firewall für die Coordinatoren (s. Coordinator zum externen Netzwerk verbinden auf S. 110) durchgeführt werden.
Tunnel (nur für Coordinator)	In dieser Registerkarte können die IP-Adressen bestimmt werden, welche von diesem Coordinator getunnelt werden (s. Tunnelung auf S. 114).
IPsec-Verbindung (nur für Coordinator)	In dieser Registerkarte können die Parameter des Coordinators in seiner Eigenschaft als IPsec-Gateway konfiguriert werden, um die Anbindung mobiler Endgeräte an das ViPNet Netzwerk zu ermöglichen (s. Konfiguration des IPsec-Profils für den Windows-Coordinator auf S. 195). Die Registerkarte **IPsec-Verbindung** wird nur dann eingeblendet, wenn eine Lizenz für den Einsatz des Coordinators als IPsec-Gateway zur Verfügung steht.

Registerkarte	Beschreibung
Netzwerkeinstellungen (nur für Coordinatoren mit dem Software ViPNet Coordinator HW/VA)	In dieser Registerkarte können die Einstellungen der Netzwerkadapter von ViPNet Coordinator HW/VA konfiguriert und zusätzliche Routen für die Weiterleitung des Traffics aus einem Subnetz in ein anderes Subnetz über den gegebenen Coordinator hinzugefügt werden (d. h. es kann die Zuordnung der Zieladressen den Netzwerkadaptern, über welche das IP-Paket geleitet wird, festgelegt werden). Die Registerkarte **Netzwerkeinstellungen** wird nur für Coordinatoren ViPNet Coordinator HW/VA angezeigt.
Verwaltete Netzwerkknoten (lediglich für den Client, auf dem das Policy Manager benutzt wird)	In dieser Registerkarte kann die Liste der verwalteten Knoten für das ViPNet Policy Manager festgelegt werden (s. Verwendung der Software ViPNet Policy Manager auf S. 120).
Profil (nur für Smartphone-Clients)	In dieser Registerkarte kann das IPsec-Profil des mobilen Geräts, das mit dem ViPNet Netzwerk verbunden werden soll, eingestellt werden (s. Profile IPsec für Smartphone-Clients einstellen auf S. 211).



Hinweis. Mit den Symbole und wird der Manager-Arbeitsplatz gekennzeichnet. Die Symbole und im Titel der Registerkarte und im Netzwerkknotennamen (in der Navigationsleiste) weisen auf unvollständige oder widersprüchliche Daten in der Konfiguration hin (s. Erkennen von Konfliktsituationen und unvollständigen Daten in der ViPNet Netzwerkkonfiguration auf S. 128)

Ordner „Partnernetzwerke“

Damit Informationen über ViPNet Partnernetzwerke angezeigt werden, mit denen Partnernetzwerk-Verbindungen bestehen, klicken Sie in der Navigationsleiste auf **Partnernetzwerke**.

Im Bereich **Partnernetzwerke** sind folgende Angaben enthalten:

- ViPNet Netzwerke, mit denen eine Verbindung aufgebaut wurde (Partnernetzwerke).
- Verfügbare Aktualisierungen der ein- und ausgehenden Partnernetzwerk-Informationen.
- Status der eingehenden Partnernetzwerk-Informationen (nicht bearbeitet, nicht angenommen, fehlt).
- Status der ausgehenden Partnernetzwerk-Informationen (nicht versendet, versendet, als Datei gespeichert).

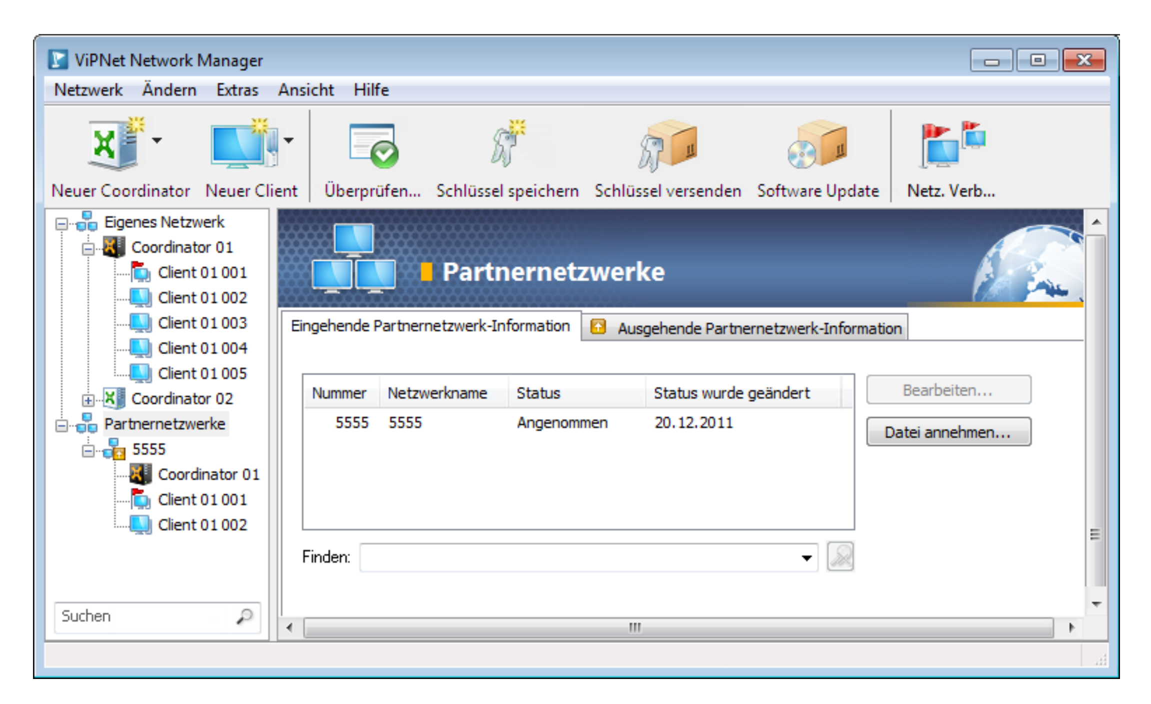


Abbildung 42. Partnernetzwerke

Über den Aufbau von Verbindungen mit anderen ViPNet Netzwerken lesen Sie im Abschnitt Partnernetzwerk-Verbindungen (auf S. 165).

Wenn in der Navigationsleiste ein Partnernetzwerk ausgewählt wird, werden in der Panel-Ansicht folgende Informationen angezeigt:

- Nummer des Partnernetzwerks.
- Name des Gateway-Coordinators des Partnernetzwerks.
- Name des Gateway-Coordinators im eigenen Netzwerk, der als Gateway für Verbindungen zum ausgewählten Partnernetzwerk eingesetzt wird.
- Das Erstellungsdatum des Partnernetzwerk-Masterschlüssels.
- Liste von Netzwerkknoten des eigenen ViPNet Netzwerks, die sich an den Partnernetzwerk-Verbindungen mit dem ausgewählten Netzwerk beteiligen.

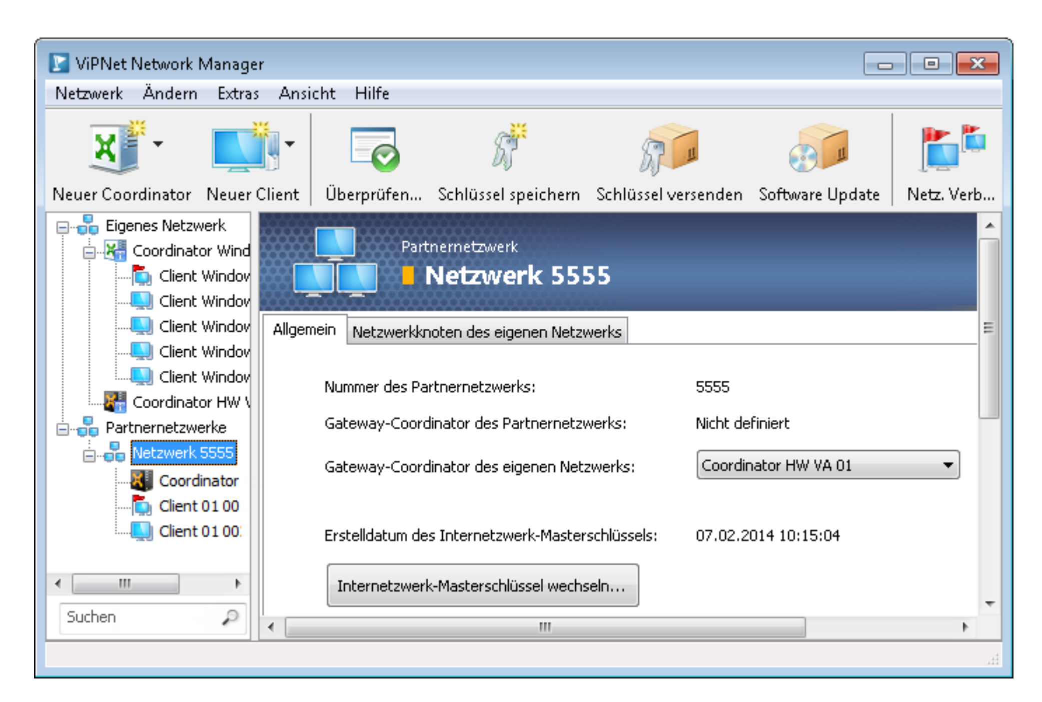


Abbildung 43. Eigenschaften des Partnernetzwerks

Änderung des Benutzerpassworts

Im Programm ViPNet Network Manager gibt es zwei Möglichkeiten, die Benutzerpasswörter zu ändern:

- Änderung des Passworts vor dem Installieren der Schlüsseldistribution auf dem Knoten. In diesem Fall wird das neue Benutzerpasswort gemeinsam mit der Schlüsseldistribution gespeichert und danach bei der Arbeit mit dem Programm ViPNet Monitor auf dem Netzwerkknoten verwendet.

  Wenn die Verwendung zufälliger Passwörter nicht erwünscht ist, dann empfehlen wir, die Benutzerpasswörter für alle Netzwerkknoten sofort nach dem Erstellen oder Ändern der ViPNet Netzwerkstruktur zu ändern.

- Änderung des Passworts nach dem Erstellen der Schlüsseldistribution. In diesem Fall wird nach dem Update der Schlüssel auf dem Netzwerkknoten eine Meldung mit der Empfehlung angezeigt, das Benutzerpasswort zu ändern. Das Passwort, das im Programm ViPNet Network Manager definiert wurde, wird nicht an den Netzwerkknoten übermittelt.

Zum Ändern des Benutzerpassworts:

1 Wählen Sie in der Navigationsleiste den Netzwerkknoten aus, für den das Benutzerpasswort geändert werden soll.

2 Klicken Sie auf der Registerkarte **Schlüssel** auf **Passwort ändern**. Es wird das Fenster **Benutzerpasswort** geöffnet.

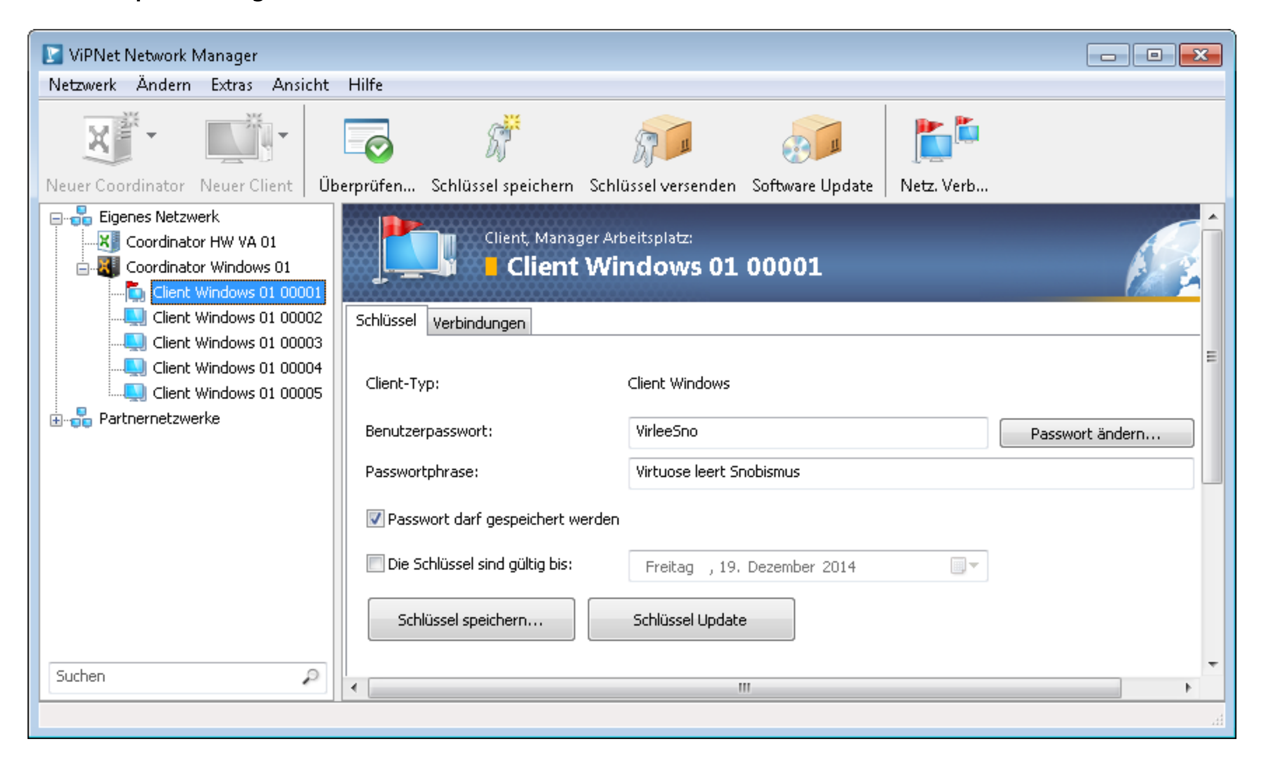


Abbildung 44. Registerkarte „Schlüssel“

3 Im Fenster **Benutzerpasswort** wird ein Zufallspasswort auf Basis der Passwortphrase erstellt.

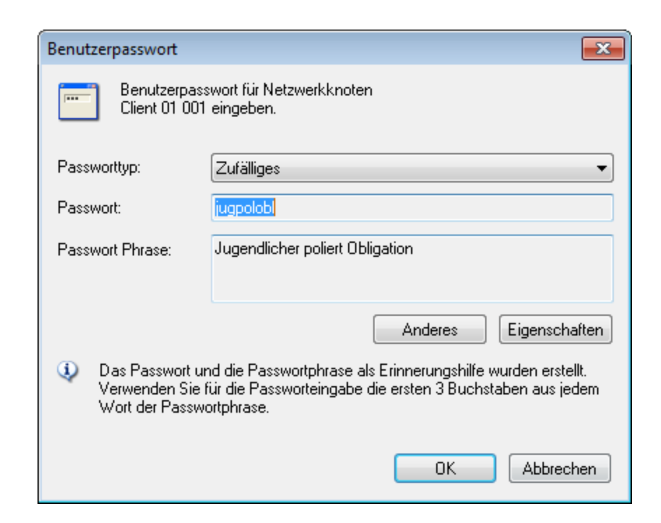


Abbildung 45. Benutzerpasswort erstellen

4 Wenn Sie ein anderes Passwort erstellen möchten:

- Klicken Sie auf **Anderes**, wenn Sie ein anderes Zufallspasswort generieren möchten.



Tipp. Wenn Sie die Parameter des Zufallspasswortes ändern möchten, klicken Sie auf **Eigenschaften**. Das Fenster **Eigenschaften zufälliger Passwörter (s.** Konfiguration der Eigenschaften der Benutzerpasswörter **auf S. 139)** wird geöffnet.

- Wenn Sie ein benutzerdefiniertes Passwort bevorzugen, wählen Sie in der Liste **Passworttyp** den Eintrag **Benutzerdefiniertes**, dann geben das gewünschte Passwort ein und bestätigen es

5 Zum Speichern des Passworts klicken Sie auf **OK**.



Konfiguration des ViPNet Netzwerks

Vorgehensweise beim Konfiguration des ViPNet Netzwerks

Die nachfolgende Tabelle soll Ihnen helfen, im Programm ViPNet Network Manager ein vollständig funktionsfähiges ViPNet Netzwerk anzulegen und zu konfigurieren, wobei manuelle Einstellungen unmittelbar auf den einzelnen Netzwerkknoten vermieden werden.



Hinweis. Wenn ein Link in der folgenden Aufgabenliste zu einem Kapitel mit allgemeinen Informationen führt, machen Sie sich mit diesen Informationen vertraut und gehen Sie dann zum nächsten Schritt über.

	Aktion	Link
☐	Erstellen Sie die Grundstruktur des ViPNet Netzwerks mit Hilfe des ViPNet Netzwerkaufbau Assistenten. Sie können die Struktur manuell im Hauptfenster von ViPNet Network Manager erstellen.	Erstellen des ViPNet Netzwerks (auf S. 86) Ändern der ViPNet Netzwerkstruktur (auf S. 89)
☐	Stellen Sie sicher, dass die vergebenen ViPNet Benutzerpasswörter den aktuellen Sicherheitsrichtlinien entsprechen. Wenn nötig, verändern Sie die Passwörter.	Änderung des Benutzerpassworts (auf S. 104)
☐	Geben Sie die Zugriffs-IP-Adressen der Coordinatoren.	Zugriffs-IP-Adressen der Coordinatoren (auf S. 109)
☐	Konfigurieren Sie die Firewall-Verbindungsparameter für die Coordinatoren.	Coordinator zum externen Netzwerk verbinden (auf S. 110)
☐	Konfigurieren Sie die Tunnelregeln auf den Coordinatoren (nach Bedarf).	Tunnelung (auf S. 114)
☐	Definieren Sie eine Liste der DNS-Server Ihres Netzwerks.	Liste der DNS-Server (auf S. 125)
☐	Stellen Sie sicher, dass die angegebenen Parameter korrekt sind und keine Konfliktsituationen verursachen.	Erkennen von Konfliktsituationen und unvollständigen Daten in der ViPNet Netzwerkkonfiguration (auf S. 128)
☐	Erstellen Sie die Schlüsseldistributionen.	Speichern der Schlüsseldistributionen (auf S. 142)
☐	Übertragen Sie die Schlüsseldistributionen auf sicherem Wege auf die Netzwerkknoten.	
☐	Installieren Sie die Schlüsseldistributionen auf den ViPNet Netzwerkknoten.	Installation der Schlüsseldistribution (auf S. 216)
☐	Wenn nötig, schließen Sie die mobilen Geräte an das	Konfiguration von IPsec-Verbindungen

	Aktion	Link
	ViPNet Netzwerk an.	mit mobilen Geräten und anderen Netzwerken (auf S. 187)
☐	Stellen Sie sicher, dass das ViPNet Netzwerk ordnungsgemäß funktioniert.	



Tipp. Wir empfehlen, die Liste auszudrucken, und die einzelnen Schritte nach ihrer Durchführung zu markieren.

Konfiguration der Coordinatoren

Zugriffs-IP-Adressen der Coordinatoren

Damit ViPNet Netzwerkknoten Verbindungen untereinander aufbauen können, sollten Zugriffs-IP-Adressen von Coordinatoren konfiguriert werden, auf denen diese Knoten registriert sind. Im Programm ViPNet Network Manager können Sie die Zugangsadressen für jeden Coordinator des Netzwerks angeben.



Achtung! Vor dem erstmaligen Erstellen der Schlüsseldistributionen für alle Netzwerkknoten sollte für jeden Coordinator zumindest eine Zugangsadresse definiert werden. Anderenfalls kann es zu Problemen mit der Funktionsfähigkeit bestimmter Typen von Clients kommen.

Als Zugangsadressen können folgende Adressen festgelegt werden:

- IP-Adressen des Coordinators;
- DNS-Namen des Coordinators;
- externe IP-Adressen der Firewall, über welche der Zugriff auf das Internet erfolgt;
- DNS-Namen der Firewall.

Anstatt der IP-Adressen (oder zusätzlich dazu) können auch die DNS-Namen der Coordinatoren angegeben werden. Die IP-Adressen der Coordinatoren erfahren Sie vom Netzwerkadministrator Ihrer Organisation.

Zum Einstellen der Liste der Zugangsadressen des Coordinators:

1 Wählen Sie den Coordinator in der Navigationsleiste aus und öffnen in der Panel-Ansicht die Registerkarte **Zugangsadressen**.

2 Führen Sie in Gruppe IP-Adressen oder DNS-Namen die erforderlichen Schritte aus:

   - Zum Hinzufügen der IP-Adresse wählen Sie einen Coordinator aus und klicken auf **Hinzufügen** in der Registerkarte **IP-Adressen**.
   - Zum Ändern der IP-Adresse eines Coordinators wählen Sie die IP-Adresse in der Liste aus und klicken auf **Ändern**.
   - Zum Löschen der IP-Adresse eines Coordinators wählen Sie die IP-Adresse in der Liste aus und klicken auf **Löschen**.

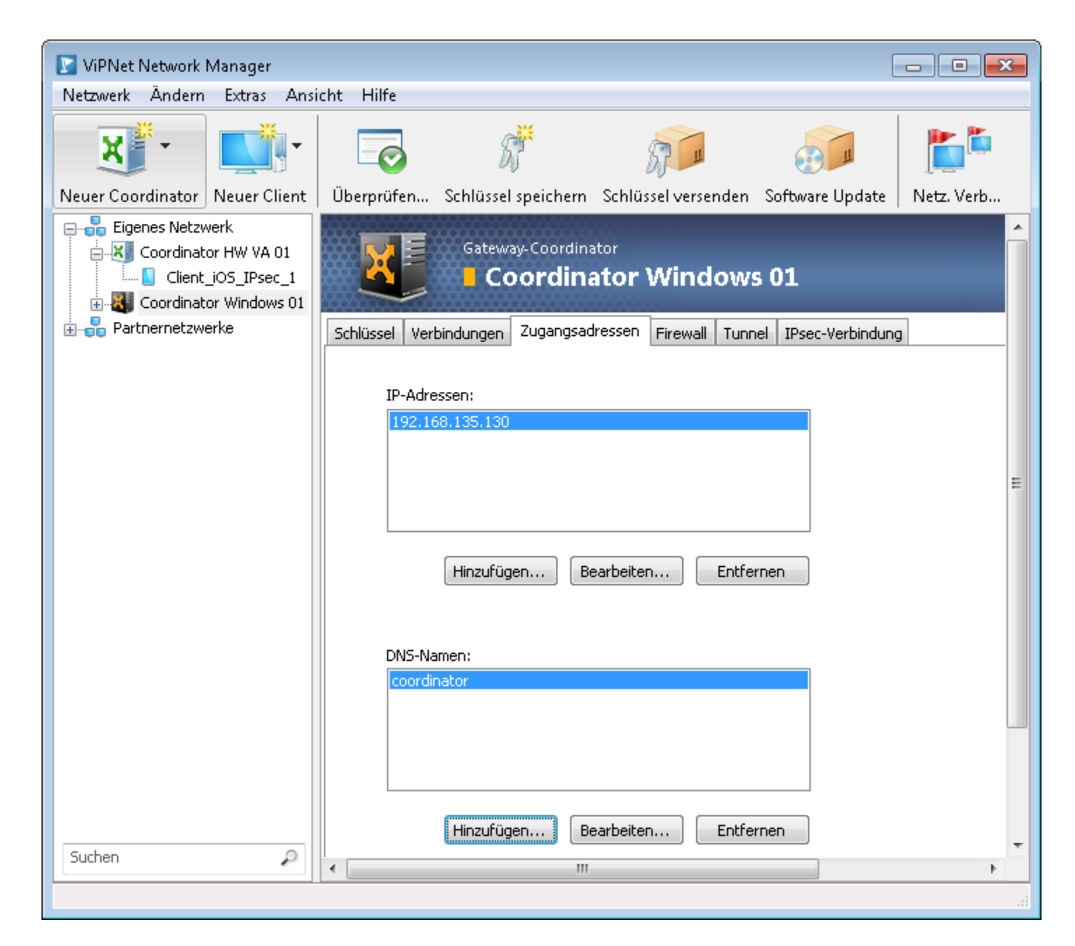


Abbildung 46. Zugriffs-IP-Adressen des Coordinators



Hinweis. Sie können einem Coordinator eine beliebige Anzahl an IP-Adressen oder DNS-Namen zuordnen. Die IP-Adressen müssen einmalig sein und dürfen nicht mit den IP-Adressen getunnelter Verbindungen übereinstimmen. Wenn Sie eine IP-Adresse oder DNS-Name eingeben, welche bereits existiert, wird Ihnen das Programm vorschlagen, eine andere Adresse zu wählen.

Coordinator zum externen Netzwerk verbinden

Wenn die Computer des lokalen Netzwerks mit externen Netzwerken kommunizieren und dazu eine beliebige Firewall oder ein anderes Gerät verwenden, das die Umsetzung von Netzwerkadressen (s. Netzwerkadressenübersetzung (NAT) auf S. 371) unterstützt, dann sollten im Programm ViPNet Network Manager entsprechende Firewall-Parameter eingestellt werden. Diese Einstellungen werden benötigt, damit Verbindungen zwischen ViPNet Netzwerkknoten und Knoten der externen Netzwerken aufgebaut werden können, ohne dass die Parameter auf den einzelnen Netzwerkknoten manuell konfiguriert werden müssen.

Informationen über die Firewall-Parameter können Sie bei den Netzwerkadministratoren Ihrer Organisation anfordern.

Wenn bei der Installation des Netzwerks für die Coordinatoren die Option **Im Hauptfenster von ViPNet Network Manager konfigurieren** oder **Verbindung über eine Firewall** ausgewählt wurde, dann wird für diese Coordinatoren standardmäßig der Verbindungsaufbau zum externen Netzwerk unter Verwendung einer Firewall mit statischem NAT festgelegt.

Wenn der Coordinator direkt (ohne Verwendung einer Firewall) mit dem externen Netzwerk verbunden ist, dann deaktivieren Sie für diesen Coordinator auf der Registerkarte **Firewall** das Kontrollkästchen **Firewall verwenden**.

Die wichtigsten Verbindungstypen, die im ViPNet Netzwerk realisierbar sind, und ihre Verwendungsmöglichkeiten auf unterschiedlichen Knoten werden im Abschnitt Konfiguration der Netzwerkverbindung der Coordinatoren (auf S. 251).

Coordinator über einen anderen Coordinator verbinden

Detaillierte Angaben über diese Verbindung finden Sie im Abschnitt Verbindung über einen Coordinator (auf S. 252).



Abbildung 47. Firewall-Typ „Coordinator“

Führen Sie die folgenden Schritte durch, um Verbindungen über einen anderen Coordinator, der als Firewall eingesetzt wird zu ermöglichen:

1. Wählen Sie in der Navigationsleiste den gewünschten Coordinator aus und öffnen in der Panel-Ansicht die Registerkarte **Firewall**.
2. Stellen Sie sicher, dass das Kontrollkästchen **Firewall verwenden** aktiviert ist.
3. Wählen Sie in der Liste **Firewall-Typ** den Eintrag **Coordinator** aus.
4. Wählen Sie aus der Liste **Coordinator, der als Firewall eingesetzt wird** den Coordinator aus, der als Firewall verwendet wird.

5 Wählen Sie aus der Liste **Positionierung des Netzwerkknotens relativ zu dem Coordinator** die Option aus, die der Konfiguration Ihres Netzwerks entspricht.



Hinweis. Diese Liste wird nur dann angezeigt, wenn sich der Coordinator, der als Firewall eingesetzt wird, ebenfalls hinter einer Firewall befindet.

Damit die gewählte Konfiguration ordnungsgemäß verwendet wird, sollten sich sowohl der Coordinator, der konfiguriert wird, als auch der Coordinator, der als Firewall eingesetzt wird, im gleichen lokalen Netzwerk befinden. Anderenfalls legen Sie als Firewall ein anderer Coordinator fest oder definieren ein anderer Firewall-Typ.

Coordinatoren über eine Firewall mit dynamischem NAT verbinden

Mehr über diese Konfiguration lesen Sie im Abschnitt Verbindung über eine Firewall mit der dynamischen Umsetzung von IP-Adressen (auf S. 253).

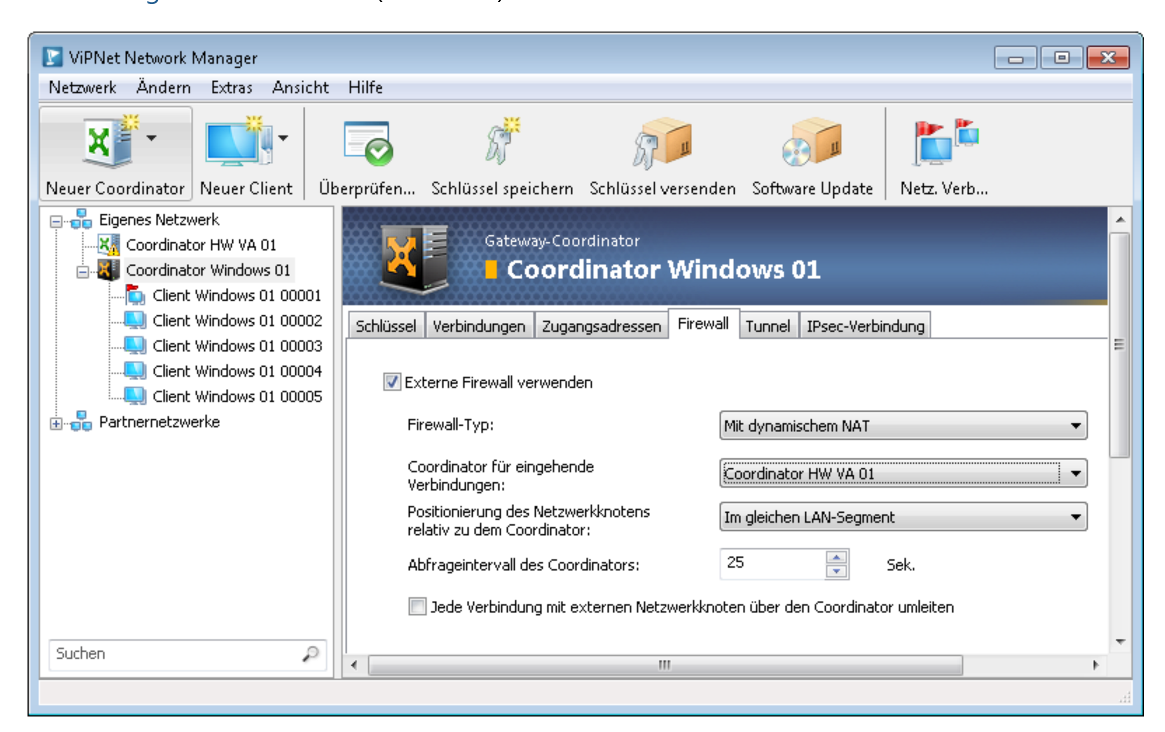


Abbildung 48. Firewall mit dynamischem NAT

Führen Sie die folgenden Schritte durch, um die Verbindung des Coordinators über eine Firewall mit dynamischem NAT zu konfigurieren:

1 Wählen Sie in der Navigationsleiste den Coordinator aus und öffnen in der Panel-Ansicht die Registerkarte **Firewall**.

2 Stellen Sie sicher, dass das Kontrollkästchen **Firewall verwenden** aktiviert ist.

3 Wählen Sie in der Liste **Firewall-Typ** den Eintrag **Mit dynamischem NAT** aus.

4 Wählen Sie in der Liste **Coordinator für eingehende Verbindungen** den Coordinator aus, der für die Weiterleitung des Traffics über die Firewall verantwortlich sein soll.



Hinweis. Dieser Coordinator sollte sich im Hinblick auf den zu konfigurierenden Coordinator in einem externen Netzwerk befinden (d. h. die beiden sollten durch eine Firewall getrennt sein). Zusätzlich sollte dieser Coordinator direkt oder über eine Firewall mit statischem NAT erreichbar sein und nicht über die gleiche Firewall funktionieren.

In der Liste sind Coordinatoren vorhanden, die Verbindungen mit dem zu konfigurierenden Coordinator haben.

5 Wenn die Liste **Positionierung des Netzwerkknotens relativ zu dem Coordinator** angezeigt wird, bedeutet das, dass ein Coordinator für eingehende Verbindungen gewählt wurde, der sich hinter einer Firewall mit dynamischem NAT oder hinter einem anderen Coordinator befindet. Führen Sie in diesem Fall einen der folgenden Schritte durch:

- Wählen Sie in der Liste **Coordinator für eingehende Verbindungen** einen anderen Coordinator aus.
- Wenn der vorhin gewählte Coordinator weiterhin eingesetzt werden soll, lassen Sie den standardmäßig ausgewählten Wert **Im gleichen LAN-Segment** unverändert.

6 Geben Sie im Feld **Abfrageintervall des Coordinators** das Abfrageintervall für eingehende Verbindungen ein, um die Weiterleitung des Traffics über die Firewall zu gewährleisten. Standardmäßig sind 25 Sekunden eingestellt. Das Abfrageintervall darf nicht länger sein als der Timeout der dynamischen Regel auf der Firewall oder auf dem NAT-Gerät. Das Timeout kann je nach verwendetem NAT-Gerät unterschiedliche Werte besitzen, beträgt aber im Regelfall mindestens 30 Sekunden.

7 Aktivieren Sie das Kontrollkästchen **Jede Verbindung mit externen Netzwerkknoten über den Coordinator umleiten**, wenn alle externen Verbindungen über den Coordinator der eingehenden Verbindungen erfolgen sollen. In diesem Fall kann sich die Geschwindigkeit des Datenaustausches verringern, es steigt aber die Stabilität der Verbindung.

Coordinatoren über eine Firewall mit statischem NAT verbinden

Detaillierte Angaben über diese Verbindung finden Sie im Abschnitt Verbindung über eine Firewall mit der statischen Umsetzung von IP-Adressen (auf S. 255).

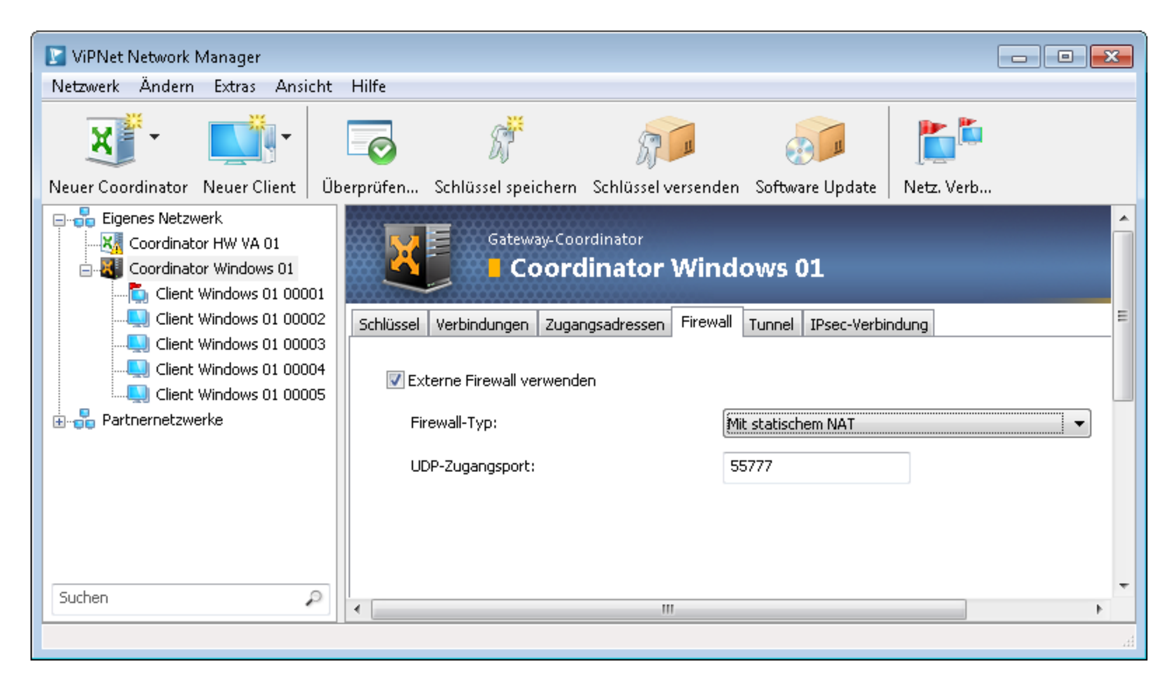


Abbildung 49. Firewall mit statischem NAT

Führen Sie die folgenden Schritte durch, um die Verbindung des Coordinators über eine Firewall mit statischem NAT zu konfigurieren:

1. Wählen Sie in der Navigationsleiste den gewünschten Coordinator aus und öffnen in der Panel-Ansicht die Registerkarte **Firewall**.
2. Stellen Sie sicher, dass das Kontrollkästchen **Externe Firewall verwenden** aktiviert ist.
3. Wählen Sie in der Liste **Firewall-Typ** den Eintrag **Mit statischem NAT** aus.
4. Ändern Sie bei Bedarf die Portnummer im Feld **UDP-Zugangsport**. Standardmäßig ist der Port 55777 eingestellt. Dieser Port wird auf der Firewall festgelegt, um den Zugang externer Knoten zum gegebenen Coordinator zu ermöglichen. Die Portnummer sollte nur dann geändert werden, wenn innerhalb des lokalen Netzwerks mehrere Netzwerkknoten über eine Firewall direkt kommunizieren sollen (d. h. auf jedem dieser Netzwerkknoten ist die Verbindung über eine Firewall mit statischem NAT eingestellt). In diesem Fall sollte für jeden dieser Netzwerkknoten eine eigene Portnummer angegeben werden.

Tunnelung

Damit Coordinatoren Verbindungen tunneln können (s. Schutz des Traffics offener Netzwerkknoten (Tunnelung) auf S. 299), sollten zunächst die IP-Adressen der Verbindungen definiert werden, die von jedem Coordinator zu tunneln sind. Zusätzlich sollte die Maximalanzahl an Verbindungen festgelegt werden, die von einem Coordinator gleichzeitig getunnelt werden können (die Tunnelung von Verbindungen sollte dabei von der Lizenz erlaubt sein).

Die Konfiguration der IP-Adressen getunnelter Verbindungen im Programm ViPNet Network Manager ermöglicht es, die Anzahl an manuellen Einstellungen auf jedem Netzwerkknoten auf ein Mindestmaß einzuschränken. Wenn die IP-Adressen getunnelter Verbindungen für alle tunnelnden Coordinatoren

nicht im Programm ViPNet Network Manager definiert werden, dann müssen diese IP-Adressen manuell auf jedem betroffenen Coordinator und auf allen darauf registrierten Netzwerkknoten eingestellt werden.

Informationen über die IP-Adressen erhalten Sie von den Administratoren Ihres Netzwerks.

Gehen Sie wie folgt vor, um für einen Coordinator die IP-Adressen oder die IP-Adressbereiche der getunnelten Verbindungen festzulegen:

1 Wählen Sie in der Navigationsleiste den Coordinator aus, auf dem die Tunnelung konfiguriert werden soll.

2 Öffnen Sie in der Panel-Ansicht die Registerkarte **Tunnel**.

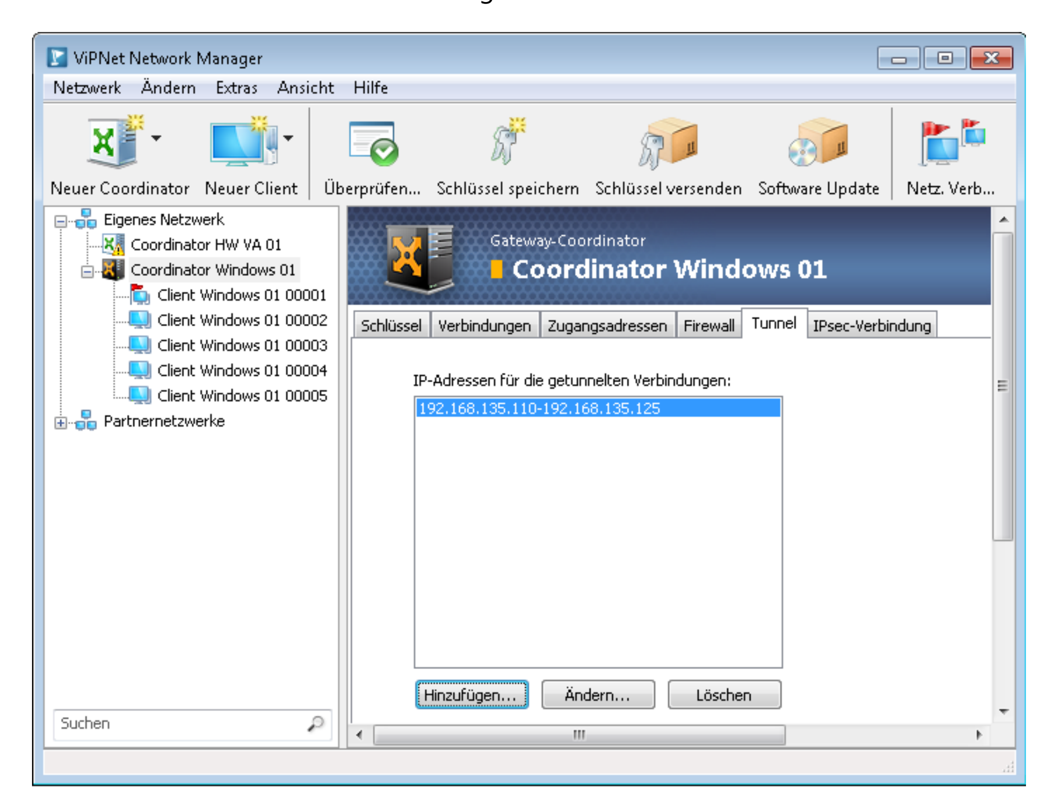


Abbildung 50. Konfiguration der getunnelten Verbindungen

3 Führen Sie erforderliche Aktionen durch:

- Zum Hinzufügen der IP-Adressen oder Adressbereiche der getunnelten Verbindungen, klicken Sie auf **Hinzufügen**.
- Zum Ändern der IP-Adresse einer getunnelten Verbindung, wählen Sie die IP-Adresse oder Adressbereich aus und klicken auf **Ändern**.
- Zum Löschen der IP-Adresse einer getunnelten Verbindung, wählen Sie die IP-Adresse oder Adressbereich aus und klicken auf **Löschen**.

Netzwerkeinstellungen von ViPNet Coordinator HW/VA

Die Netzwerkeinstellungen für die Coordinatoren ViPNet Coordinator Windows werden mit Hilfe der integrierten Werkzeuge von Windows unmittelbar auf den Knoten durchgeführt. Für ViPNet Coordinator HW/VA-Coordinatoren werden diese Einstellungen manuell mit Hilfe der Konsole oder über die Webschnittstelle für jeden Coordinator gesondert konfiguriert. Um die Aufgaben des Netzwerkadministrators zu vereinfachen, können folgende Netzwerkeinstellungen für die ViPNet Coordinator HW/VA-Coordinatoren zentralisiert im Programm ViPNet Network Manager durchgeführt werden:

- Konfiguration der Ethernet-Netzwerkadapter. Für jeden Adapter werden die Netzwerk-Verbindungseinstellungen (entweder automatisch oder manuell) und die zusätzlichen IP-Adressen (bei Bedarf) definiert.
- Standardroute (Standardgateway) und zusätzliche Routen für die Weiterleitung des Traffics. Das Routing bestimmt den Weg der IP-Pakete von einem Netzwerk in ein anderes Netzwerk über den Coordinator ViPNet Coordinator HW/VA. Dieser Weg hängt von der Routingtabelle ab, die auf dem Coordinator gespeichert ist. Diese Tabelle enthält Routen, die auf allen Netzwerkadaptern automatisch hinzugefügt wurden, sowie Routen, die vom Benutzer definiert wurden (zusätzliche Routen). Auf Basis der Routingtabelle wird die Zuordnung zwischen den Zieladressen der IP-Pakete und den Netzwerkadaptern, über welche diese Pakete gesendet werden sollen, ermittelt.

Die durchgeführten Einstellungen werden dann als Teil eines Schlüsselupdates an ViPNet Coordinator HW/VA weitergeleitet.

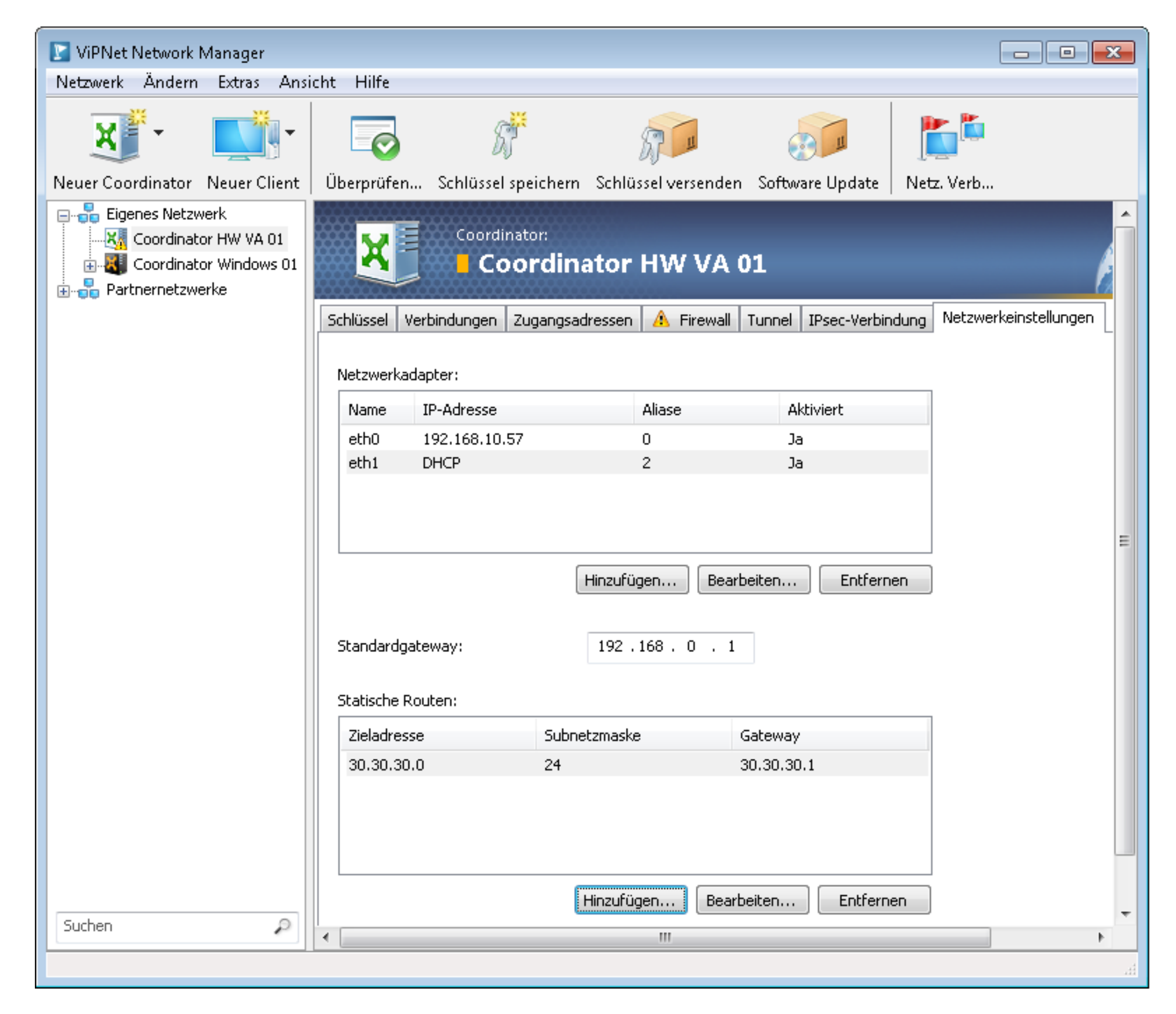


Abbildung 51. Netzwerkeinstellungen von ViPNet Coordinator HW/VA

Führen Sie die folgenden Schritte aus, um den ViPNet Coordinator HW/VA-Coordinator zu konfigurieren:

1 Wählen Sie den benötigten Coordinator in der Navigationsleiste aus und öffnen die Registerkarte **Netzwerkeinstellungen** in der Panel-Ansicht.



Hinweis. Die Registerkarte **Netzwerkeinstellungen** wird nur für Coordinatoren ViPNet Coordinator HW/VA angezeigt.

---

2 Konfigurieren Sie die Liste der Netzwerkadapter. Dazu:

2.1 Klicken Sie in Gruppe **Netzwerkadapter** auf die Schaltfläche **Hinzufügen**.

2.2 Aktivieren Sie im Fenster **Netzwerkadapter** das Kontrollkästchen **Adapter auf dem Gerät aktivieren**, damit der Adapter beim Start von ViPNet Coordinator HW/VA aktiviert wird. Wenn dieses Kontrollkästchen nicht aktiviert wird, dann wird sich der gewählte Netzwerkadapter im Reservemodus befinden, sodass Sie ihn jederzeit aktivieren können. Diese Funktion kann dann verwendet werden, wenn Sie die Durchführung der Adapterkonfiguration nicht abgeschlossen haben, ViPNet Coordinator HW/VA jedoch neu gestartet werden muss.

2.3 Wählen Sie den Namen des Netzwerkadapters in der entsprechenden Liste aus. Den auf dem ViPNet Coordinator HW/VA-Coordinator installierten Ethernet-Netzwerkadaptern werden die Namen `eth0`, `eth1` u. s. w. (je nach Anzahl der Adapter im System) zugewiesen.

2.4 Wählen Sie in Gruppe **Abrufen der IP-Adresse und anderer Parameter** eine der folgenden Optionen aus:

- **Statische IP-Adresse verwenden**, um dem Adapter eine statische IP-Adresse zuzuordnen. Geben Sie in diesem Fall die IP-Adresse und die Subnetzmaske an.
- **Automatisch**, um die Verbindungseinstellungen vom DHCP-Server zu erhalten. Aktivieren oder deaktivieren Sie in diesem Fall das Kontrollkästchen **Standardgateway vom DHCP-Server beziehen**. Da es nur ein Standardgateway geben kann, sollte dieses Kontrollkästchen nur für einen der vorhandenen Adapter aktiviert werden. Für alle anderen Adapter sollte das Kontrollkästchen **Standardgateway vom DHCP-Server beziehen** automatisch deaktiviert werden.

2.5 Fügen Sie bei Bedarf zusätzliche IP-Adressen (Aliase) auf dem Adapter mit Hilfe der Schaltfläche **Hinzufügen** hinzu. Zusätzliche IP-Adressen ermöglichen die Unterteilung des physischen Netzwerks in unterschiedliche logische Netzwerke bei Verwendung desselben Ethernet-Adapters. Diese Funktion kann z. B. dann nützlich sein, wenn auf dem ViPNet Coordinator HW/VA-Coordinator nur ein Netzwerkadapter zur Verfügung steht.

2.6 Klicken Sie nach der Durchführung der Einstellungen des Netzwerkadapters auf **OK**.

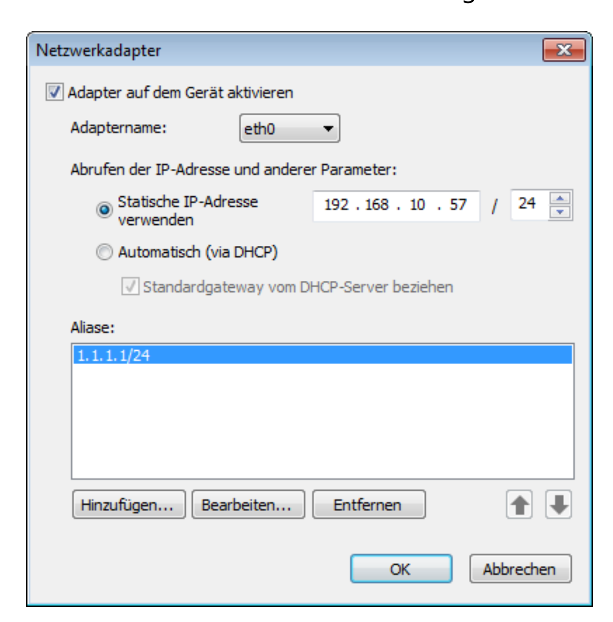


Abbildung 52. Parameter des Netzwerkadapters

3 Geben Sie im Feld **Standardgateway** die IP-Adresse des Standardgateways ein. An dieses Standardgateway werden alle IP-Pakete weitergeleitet, für welche keine Route mit Hilfe der Routingtabelle ermittelt werden kann.

4 Definieren Sie die Liste der zusätzlichen Routen, die zur Routingtabelle von ViPNet Coordinator HW/VA hinzugefügt werden sollen. Dazu:

4.1 Klicken Sie in Gruppe **Andere Routen** auf die Schaltfläche **Hinzufügen**.

4.2 Geben Sie im Fenster **Statische Route** IP-Adresse und die Subnetzmaske des Zielnetzwerks sowie das Gateway für den Zugang zum Subnetz in den entsprechenden Feldern an. Der Netzwerkadapter der gegebenen Route wird dabei automatisch ermittelt.

4.3 Klicken Sie auf die Schaltfläche **OK**.

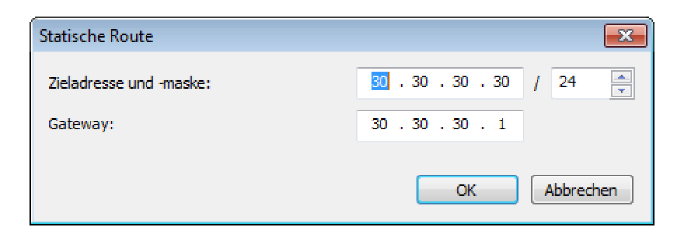


Abbildung 53. Routenparameter

Wählen Sie zum Bearbeiten der Routenliste den benötigten Namen in der Liste aus und klicken Sie auf die Schaltfläche **Bearbeiten** oder **Entfernen**.

Versenden Sie nach der Durchführung der erforderlichen Coordinatoreinstellungen Schlüsselupdates an alle Netzwerkknoten.

Konfiguration der Clients

Verwendung der Software ViPNet StateWatcher

Beim Bearbeiten der Netzwerkstruktur im Netzwerkaufbau-Assistenten (s. Ändern der ViPNet Netzwerkstruktur auf S. 89) und bei der anschließenden Konfiguration des Netzwerks im Programm ViPNet Network Manager können Sie die Verwendung von ViPNet StateWatcher auf einem beliebigen Client vom Typ ViPNet Client Windows erlauben.

Führen Sie die folgenden Schritte aus, um die Verwendung von ViPNet StateWatcher auf einem Netzwerkclient zuzulassen:

1 Klicken Sie im Hauptfenster von ViPNet Network Manager in der Navigationsleiste mit der rechten Maustaste auf den Client, dem die Verwendung des Programms ViPNet StateWatcher erlaubt werden soll.

2 Wählen Sie im Kontextmenü den Eintrag **StateWatcher zulassen**.

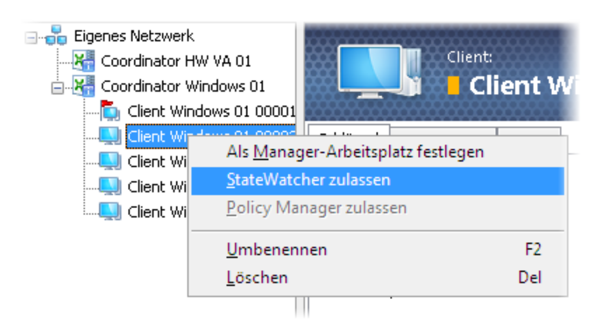


Abbildung 54. Verwendung der Software ViPNet StateWatcher erlauben

3 Erstellen Sie neue Schlüsseldistributionen und versenden sie an alle Knoten des Netzwerks (s. Versenden der Schlüssel-Updates auf S. 145).

Nun können die Benutzer mit dem Programm ViPNet StateWatcher auf dem gegebenen Client arbeiten, das Symbol dieses Clients in der Navigationsleiste wird dabei auf geändert.

Verwendung der Software ViPNet Policy Manager

Beim Bearbeiten der Netzwerkstruktur im Netzwerkaufbau-Assistenten (s. Ändern der ViPNet Netzwerkstruktur auf S. 89) und bei der anschließenden Konfiguration des Netzwerks im Programm ViPNet Network Manager können Sie die Verwendung von ViPNet Policy Manager auf einem beliebigen Client vom Typ ViPNet Client Windows erlauben.

Führen Sie die folgenden Schritte aus, um die Verwendung von ViPNet Policy Manager auf einem Netzwerkclient zuzulassen:

1 Klicken Sie im Hauptfenster von ViPNet Network Manager in der Navigationsleiste mit der rechten Maustaste auf den Client, dem die Verwendung des Programms ViPNet PolicyManager erlaubt werden soll.

2 Wählen Sie im Kontextmenü den Eintrag **Policy Manager zulassen**.

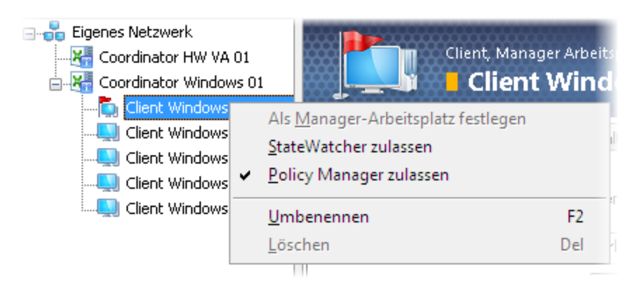


Abbildung 55. Verwendung der Software ViPNet Policy Manager erlauben

3 Öffnen Sie in der Panel-Ansicht die Registerkarte **Verwaltete Netzwerkknoten** und legen die Liste der Netzwerkknoten Ihres Netzwerkes fest, für die Sie die Sicherheitslinien im Programm ViPNet Policy Manager konfigurieren können:

- Fügen Sie die Netzwerkknoten mit Hilfe der Schaltfläche **Hinzufügen** in die Liste hinzu.



Hinweis. Unter der Liste der verwalteten Netzwerkknoten sind die maximale in der Lizenz erlaubte Anzahl der verwalteten Knoten sowie die Anzahl der hinzugefügten Knoten angegeben.

- Um die ausgewählten Knoten aus der Liste zu entfernen, benutzen Sie die Schaltfläche **Entfernen**.

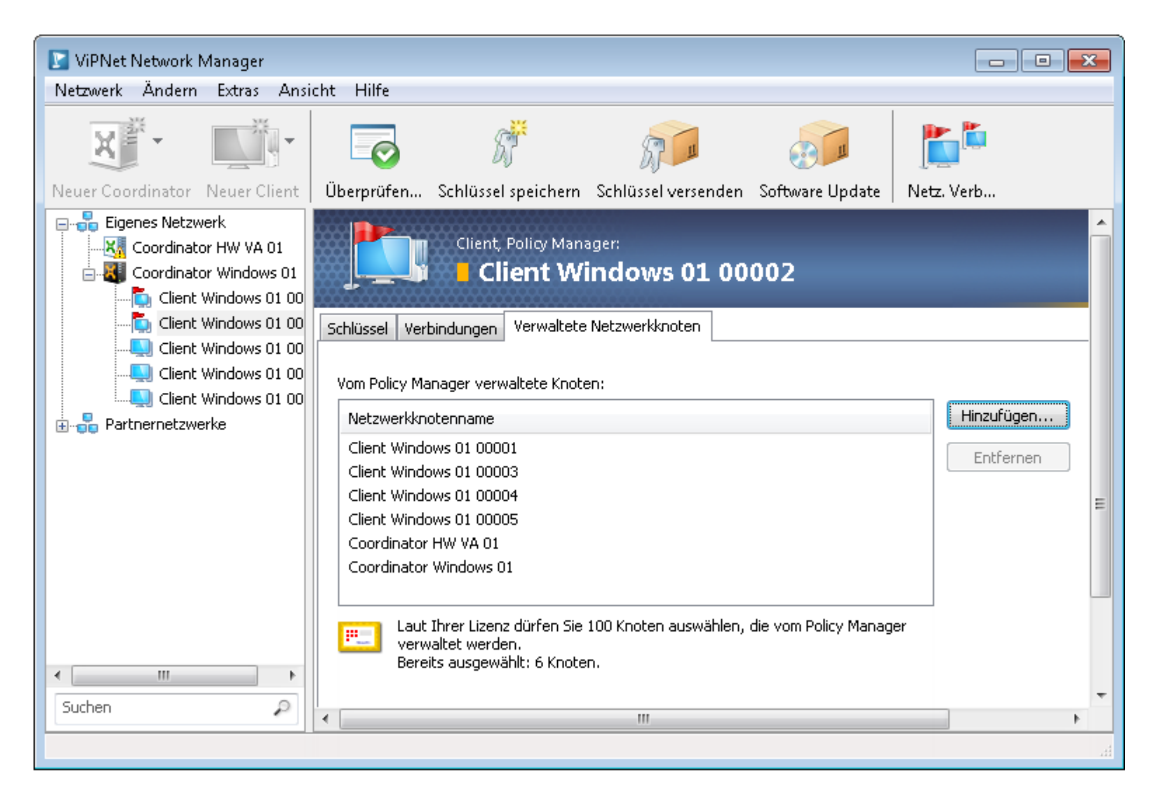


Abbildung 56. Liste verwalteter Knoten

4 Erstellen Sie neue Schlüsseldistributionen und versenden sie an alle Knoten des Netzwerks (s. Versenden der Schlüssel-Updates auf S. 145).

Nun können die Benutzer mit dem Programm ViPNet Policy Manager auf dem gegebenen Client arbeiten, das Symbol dieses Clients in der Navigationsleiste wird dabei auf geändert.

Verwendung zusätzlicher ViPNet Komponenten

Bei der Verteilung von Lizenzeinschränkungen wird festgelegt, ob zusätzliche ViPNet Software und Funktionen verwendet werden können. Sie könnten folgende zusätzliche Komponenten für die Verwendung auf den Netzwerkknoten erlauben:

- ViPNet Business Mail für Netzwerknoten mit ViPNet Client für Windows.
- ViPNet SafeDisk-V für Netzwerkknoten mit ViPNet Client für Windows.
- ViPNet Connect für Netzwerkknoten mit ViPNet Client für Windows, ViPNet Client für Android, ViPNet Client für Mac OS X.
- ViPNet Failover für Knoten ViPNet Coordinator HW/VA.

Bei der Verteilung von Lizenzeinschränkungen bestimmt das Programm ViPNet Network Manager automatisch die Kompatibilität zwischen der zusätzlichen ViPNet Komponente und den Knotentypen, auf denen diese Komponente verwendet werden soll.

Um die Lizenzeinschränkungen für eine zusätzliche ViPNet Komponente zu verteilen, führen Sie folgende Schritte aus:

1. Wählen Sie den Bereich **Eigenes Netzwerk** im Hauptfenster des Programms ViPNet Network Manager.
2. Wählen Sie in der Panel-Ansicht die Registerkarte **Allgemeines**. Dabei wird der Inhalt Ihrer Lizenz für das ViPNet Netzwerk angezeigt.
3. Klicken Sie in der Gruppe Anwendungen und zusätzliche Funktionen auf die Zeile mit der Komponente, deren Verwendung Sie für diese oder andere Knoten erlauben möchten.
4. Im geöffneten Fenster wird die Liste der Netzwerkknoten, auf denen das ausgewählte Programm und die Funktion verwendet werden können, angezeigt. Aktivieren Sei die Kontrollkästchen neben den benötigten Knoten und klicken auf die Schaltfläche **OK**.

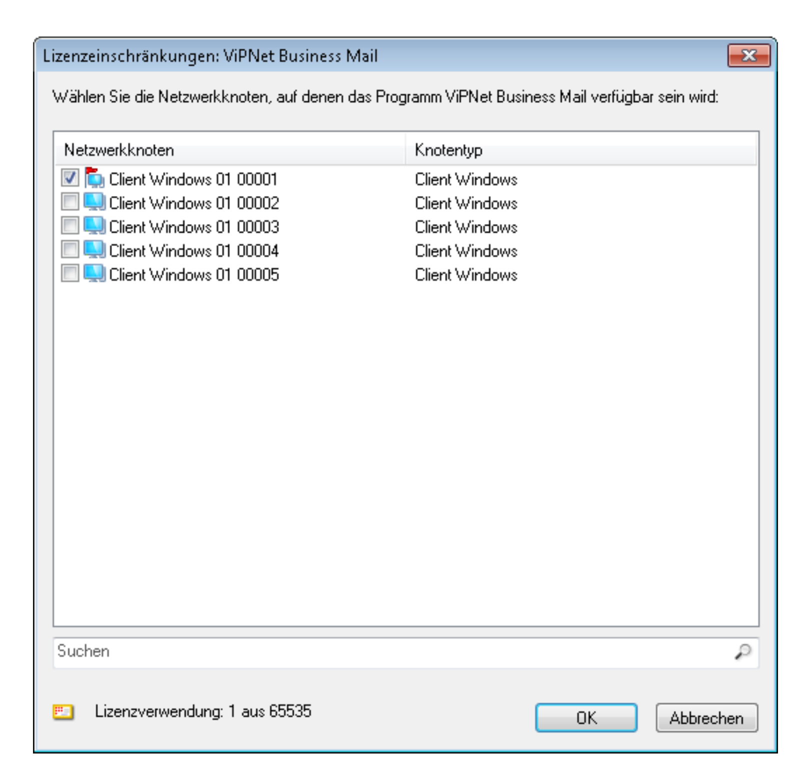


Abbildung 57. Verteilung von Lizenzeinschränkungen für die Verwendung des Programms ViPNet Business Mail

Liste der DNS-Server

Im ViPNet Netzwerk kann man DNS-Namen verwenden, um an Netzwerkknoten zu verbinden. Wenn die Anwendungen einen DNS-Namen für einen ViPNet Netzwerkknoten benutzen, dann kontaktieren sie einen DNS-Server für IP-Adresse, die diesem DNS-Namen entspricht.

Die Liste der im ViPNet Netzwerk verwendeten DNS-Server kann im Programm ViPNet Network Manager oder auf jedem Netzwerkknoten gesondert definiert werden (s. Konfiguration und Verwendung der Namensdienste DNS und WINS im ViPNet Netzwerk auf S. 305). Wenn die Liste der DNS-Server zentralisiert eingestellt wird, dann wird sie zusammen mit den Schlüsseln an die Netzwerkknoten weitergeleitet. In diesem Fall, sollen die Benutzer keine zusätzliche Aktionen durchzuführen. Wenn Sie die Einstellungen der DNS-Server ändern, dann werden sie auch zusammen mit den Schlüsseldistributionen weitergeleitet.

Mit Hilfe des Programms ViPNet Network Manager können folgende Arten von Knoten zur Liste der DNS-Server hinzugefügt werden:

- ViPNet Coordinator (Windows);
- ViPNet Coordinator HW/VA;
- ViPNet Client (Windows);
- Getunnelte Knoten.

Führen Sie die folgenden Schritte durch, um die Liste der DNS-Server des Netzwerks einzustellen:

1. Wählen Sie im Hauptfenster des Programms ViPNet Network Manager in der Navigationsleiste den Stammeintrag **Eigenes Netzwerk**.
2. Öffnen Sie in der Panel-Ansicht die Registerkarte **DNS-Server**.
3. Konfigurieren Sie die Liste der DNS-Server:
   - Klicken Sie zum Hinzufügen eines DNS-Servers aus der Liste der Netzwerkknoten auf die Schaltfläche **ViPNet Knoten hinzufügen**, wählen den benötigten Knoten im eingeblendeten Fenster Hinzufügen von ViPNet Knoten in der Liste aus und klicken auf **OK**.
   - Klicken Sie zum Hinzufügen eines getunnelten Knotens zur Liste der DNS-Server auf die Schaltfläche **Getunnelte IP-Adresse hinzufügen**, geben die IP-Adresse des getunnelten Knotens im eingeblendeten Fenster **IP-Adresse** ein und klicken dann auf **OK**.
   - Klicken Sie zum Entfernen eines Knotens aus der Liste der DNS-Server auf die Schaltfläche **Löschen**.
4. Nach Beenden des Einstellungsprozess versenden Sie Schlüssel an allen Netzwerkknoten.

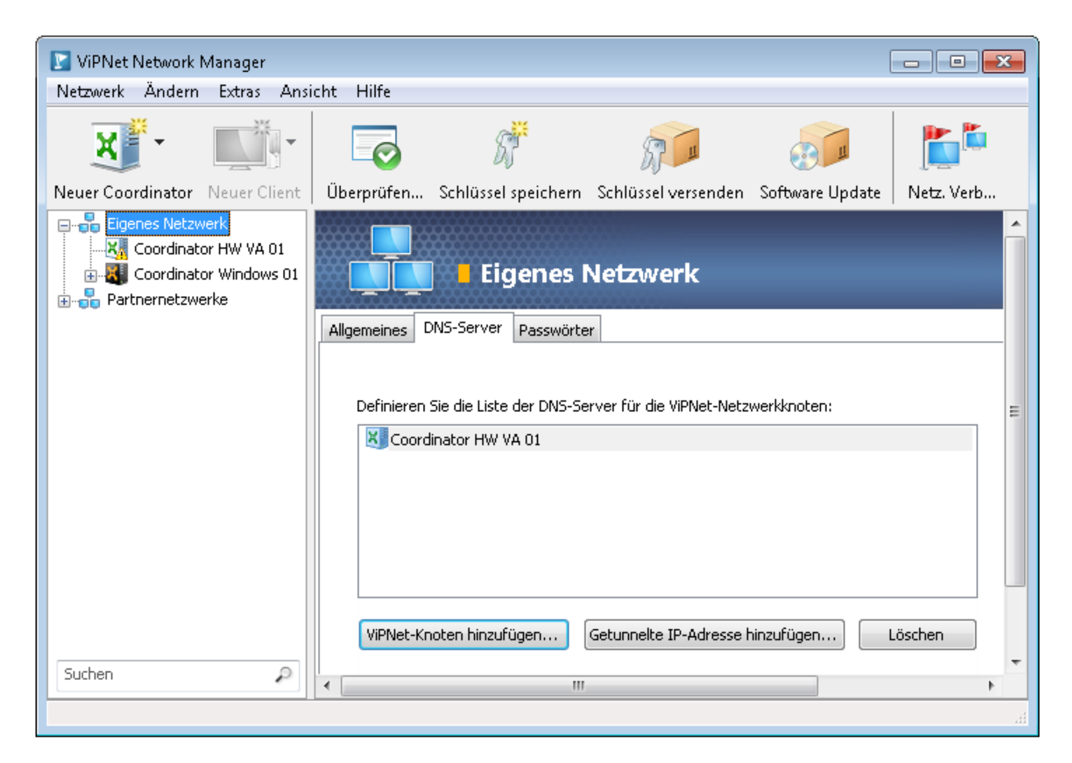


Abbildung 58. Liste der DNS-Server einstellen

Die Liste der DNS-Server ist nun eingestellt.

Speichern des Benutzerpasswortes in der Registry

Auf der Registerkarte **Schlüssel** können Sie das Speichern des Benutzerpasswortes in der Windows-Registry erlauben oder verbieten. Wenn das Speichern des Passwortes erlaubt ist, kann der Benutzer beim Start des Programms ViPNet Monitor das Passwort eingeben und das Kontrollkästchen **Passwort speichern** aktivieren. Beim nächsten Programmstart wird das Passwort automatisch im Eingabefeld eingefügt. Das Speichern des Passwortes ist beim Remotezugriff auf den Netzwerkknoten über das Programm Remote Desktop Connection (oder über ähnliche Software) nützlich, weil der Computer dadurch neu gestartet werden kann.

Wenn Sie das Speichern des Passwortes erlauben oder verbieten möchten, aktivieren oder deaktivieren Sie das Kontrollkästchen **Passwort darf gespeichert werden**:

- Wenn das Kontrollkästchen **Passwort darf gespeichert werden** aktiviert ist, kann beim Start des Programms ViPNet Monitor im Fenster zur Eingabe des Benutzerpassworts das Kontrollkästchen **Passwort speichern** aktiviert werden. Standardmäßig ist das Kontrollkästchen im Fenster der Passworteingabe aktiviert.

  Im Fenster **Sicherheitseinstellungen** wird dabei das Kontrollkästchen **Passwort darf in der Registry gespeichert werden** als aktiviert und blockiert angezeigt, auch dann, wenn Sie sich als Administrator eingeloggt haben (s. Arbeiten mit Administratorrechten auf S. 338).

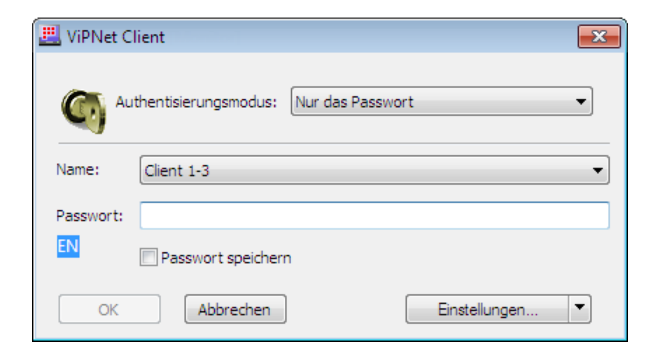
  

  Abbildung 59. Anmeldefenster des Programms

- Wenn das Kontrollkästchen **Passwort darf gespeichert werden** deaktiviert ist, ist das Speichern des Benutzerpassworts beim Start des Programms ViPNet Monitor nicht möglich. Im Fenster **Sicherheitseinstellungen** wird dabei das Kontrollkästchen **Passwort darf in der Registry gespeichert werden** als deaktiviert und blockiert angezeigt, auch dann, wenn Sie sich als Administrator angemeldet haben.

Erkennen von Konfliktsituationen und unvollständigen Daten in der ViPNet Netzwerkkonfiguration

Während der Erstellung der Struktur und der Konfiguration des ViPNet Netzwerkes erkennt das Programm ViPNet Network Manager automatisch Konfliktsituationen und unvollständig definierte Netzwerkparameter.

Daten gelten als unvollständig, falls weitere manuelle Einstellungen unmittelbar auf den ViPNet Netzwerkknoten erforderlich sind. Es ist empfehlenswert, alle erforderlichen Einstellungen der Netzwerkknoten im Programm ViPNet Network Manager durchzuführen. Dadurch kann der Vorgang der ViPNet Netzwerkinstallation wesentlich vereinfacht und beschleunigt werden. Die Konfiguration aller Parameter sollte im Programm ViPNet Network Manager vor der Installation der ViPNet Software auf den einzelnen Netzwerkknoten erfolgen.



Hinweis. Die Überprüfung der Datenvollständigkeit durch das Programm ViPNet Network Manager kann auch deaktiviert werden (s. Erkennen von unvollständigen Daten deaktivieren auf S. 130).

Die Überschriften der Registerkarten und die Namen der Netzwerkknoten (in der Navigationsleiste), deren Einstellungen unvollständige oder widersprüchliche Daten beinhalten, werden durch das Symbol für unvollständige oder widersprüchliche Daten gekennzeichnet. Ein und dasselbe Element kann gleichzeitig unvollständige und widersprüchliche Daten enthalten.

Wenn Sie detaillierte Informationen über eine bestimmte Konfliktsituation oder über unvollständige Daten erhalten möchten:

1 Öffnen Sie die Registerkarte, welche mit dem Symbol oder gekennzeichnet ist.

2 Klicken Sie in der Registerkarte auf das Symbol oder .

3 Es wird das Fenster **Überprüfung der ViPNet Netzwerkkonfiguration** geöffnet.

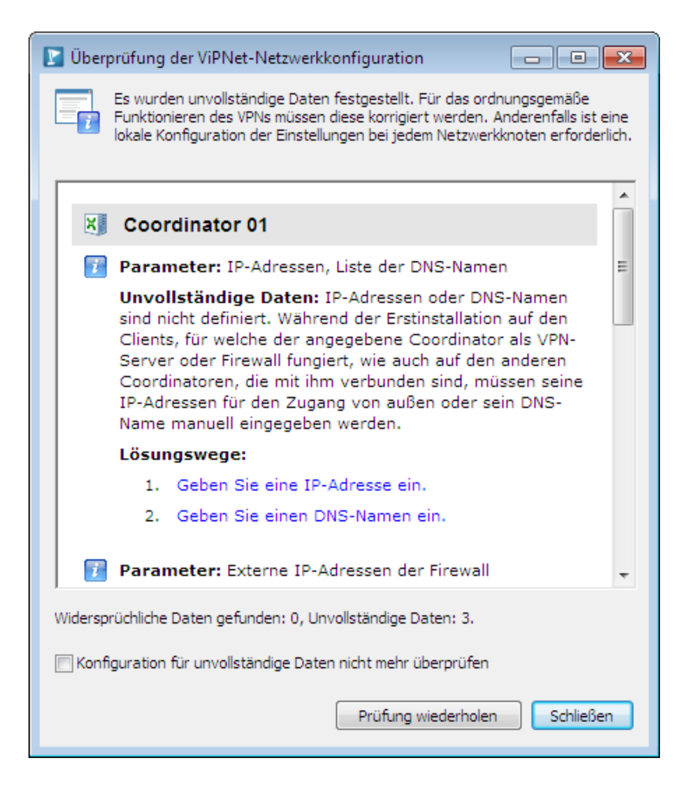


Abbildung 60. Unvollständige Daten wurden festgestellt

4 Um das Problem zu beheben, klicken Sie der Reihe nach auf die Links unter der Überschrift **Lösungswege**. Beim Klicken werden Fenster geöffnet, in denen Sie die erforderlichen Parameterwerte eingeben.

5 Nachdem alle erforderlichen Änderungen vorgenommen wurden, kehren Sie zum Fenster **Überprüfung der ViPNet Netzwerkkonfiguration** zurück und klicken auf **Prüfung wiederholen**, um festzustellen, ob das Problem behoben wurde.

Vor dem Erstellen von Schlüsseldateien für die Netzwerkknoten wird zuerst eine Gesamtüberprüfung der Netzwerkkonfiguration vorgenommen. Wenn beim Überprüfen der Konfiguration unvollständige Daten erkannt werden, können Sie durch Klicken auf die Schaltfläche **Überspringen** das Erstellen der Schlüsseldistributionen fortsetzen. Nach der Installation der ViPNet Software auf den Netzwerkknoten werden jedoch unvollständige Daten unmittelbar auf jedem Netzwerkknoten eingegeben sein. Wenn Konfliktsituationen in der Netzwerkkonfiguration festgestellt werden, können solange keine Schlüsseldistributionen für die Netzwerkknoten erstellt werden, bis alle Probleme gelöst sind.

Wenn Sie eine vollständige Liste aller Konfliktsituationen und unvollständigen Daten in der Konfiguration des ViPNet Netzwerks anzeigen möchten:

1 Klicken Sie in der Symbolleiste auf die Schaltfläche **Konfiguration überprüfen** auf oder wählen im Menü **Extras** den Befehl **Konfiguration überprüfen**.

2 Das Fenster **Überprüfung der ViPNet Netzwerkkonfiguration** wird geöffnet.

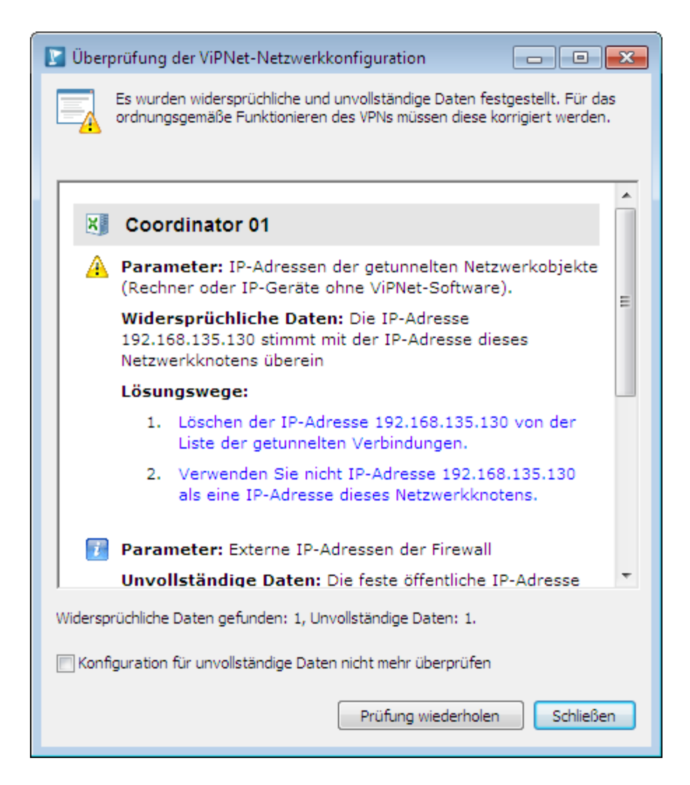


Abbildung 61. Widersprüchliche und unvollständige Daten wurden festgestellt

3 Beheben Sie alle Konflikte mit Hilfe der Links unter der Überschrift **Lösungswege**, wie weiter oben beschrieben wurde.

Erkennen von unvollständigen Daten deaktivieren

Wenn Sie ein erfahrener ViPNet Netzwerkadministrator sind, dann können Sie die Überprüfung der Datenvollständigkeit deaktivieren, um z. B. keine Benachrichtigungen über unvollständige Daten mehr zu erhalten. Das Deaktivieren der Überprüfung auf Datenvollständigkeit hat keinen Einfluss auf die Funktion der Erkennung widersprüchlicher Daten und Konfliktsituationen.

Damit die Überprüfung unvollständiger Daten deaktiviert wird, führen Sie im Programm ViPNet Network Manager eine der folgenden Aktionen aus:

- Deaktivieren Sie im Fenster **Einstellungen** im Bereich **Passwörter** das Kontrollkästchen **Konfiguration für unvollständige Daten automatisch überprüfen**.

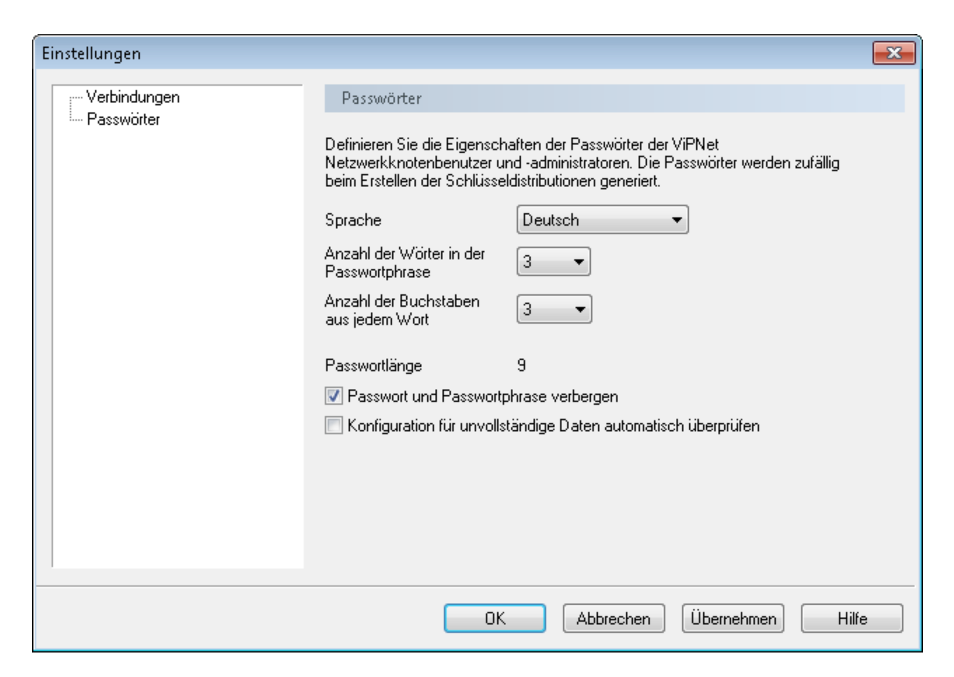


Abbildung 62. Deaktivieren der Prüfung unvollständiger Daten im Fenster „Einstellungen“

- Aktivieren Sie im Fenster **Überprüfung der ViPNet Netzwerkkonfiguration** (s. Abbildung 61 auf S. 130) das Kontrollkästchen Datenvollständigkeit nicht mehr überprüfen.

Dadurch wird die Prüfung auf Vollständigkeit der Daten deaktiviert, im Fenster **Überprüfung der ViPNet Netzwerkkonfiguration** werden nur Daten über mögliche Konfliktsituationen (falls vorhanden) angezeigt.

Ändern der Netzwerkstruktur

Bei Bedarf können folgende Änderungen an der Netzwerkstruktur im Programm ViPNet Network Manager vorgenommen werden:

- Netzwerkknoten hinzufügen;
- Netzwerkknoten umbenennen;
- Netzwerkknoten löschen;



Achtung! Das Löschen des Coordinators führt dazu, dass alle Clients, die auf diesem Coordinator registriert sind, ebenfalls gelöscht werden.

Der Netzwerkknoten, der als Arbeitsstation des ViPNet Netzwerkadministrators festgelegt wurde, und der Coordinator, auf dem dieser Netzwerkknoten registriert ist, können nicht gelöscht werden.

- Clients einem anderen Coordinator zuordnen;
- Verbindungen zwischen Netzwerkknoten ändern.



Achtung! Nach einer Änderung der Netzwerkstruktur müssen die Schlüsseldistributionen neu erstellt werden (s. Speichern der Schlüsseldistributionen auf S. 142). Wenn außerdem Partnernetzwerk-Verbindungen zu anderen ViPNet Netzwerken existieren, sollte nach einer Änderung in der Netzwerkkonfiguration überprüft werden, ob ausgehende Partnernetzwerk-Informationen erstellt wurden. Falls diese Daten erstellt wurden, leiten Sie diese an den Administrator des entsprechenden Partnernetzwerks weiter (s. Durchführen von Änderungen im eigenen Netzwerk auf S. 176).

Netzwerkknoten hinzufügen



Hinweis. Wenn die Anzahl der erstellten Netzwerkknoten die von der Lizenz erlaubte Anzahl übersteigt, können keine neuen Netzwerkknoten mehr hinzugefügt werden.

Führen Sie die folgenden Schritte durch, um einen neuen Netzwerkknoten hinzuzufügen:

1 Führen Sie eine der folgende Aktionen durch:

  - Wenn Sie einen Coordinator hinzufügen möchten, wählen Sie in der Navigationsleiste das Element **Eigenes Netzwerk** aus, klicken Sie auf die Schaltfläche **Coordinator hinzufügen** und wählen den benötigten Typ des neuen Coordinators aus.

- Wenn Sie einen neuen Client zum Coordinator hinzufügen möchten, wählen Sie diesen Coordinator in der Navigationsleiste aus, klicken in der Symbolleiste auf die Schaltfläche **Client hinzufügen** und wählen den benötigten Typ des neuen Clients aus.
- Wenn Sie einen neuen Smartphone-Client zum Coordinator hinzufügen möchten, wählen Sie diesen Coordinator in der Navigationsleiste aus, klicken in der Symbolleiste auf die Schaltfläche **Client hinzufügen** und wählen den Clienttyp **Client iOS IPsec** oder **Client Android** aus.



Hinweis. Clients vom Typ Client iOS IPsec können nur auf einem Coordinator hinzugefügt werden, der als IPsec-Gateway eingerichtet ist.

---

2 Wenn im Fenster **Einstellungen** im Bereich **Verbindungen** (s. Verbindungstypen für neue Netzwerkknoten konfigurieren auf S. 134) das Kontrollkästchen **Beim Erstellen neuer Netzwerkknoten nachfragen** aktiviert ist, dann wird beim Hinzufügen eines Coordinators oder eines Clients das Fenster **Verbindungen** geöffnet:

- Wählen Sie dort den gewünschten Verbindungstyp.
- Wenn der gewählte Verbindungstyp in Zukunft für alle neuen Netzwerkknoten automatisch festgelegt werden soll, aktivieren Sie das Kontrollkästchen **Für alle neuen Netzwerkknoten**.

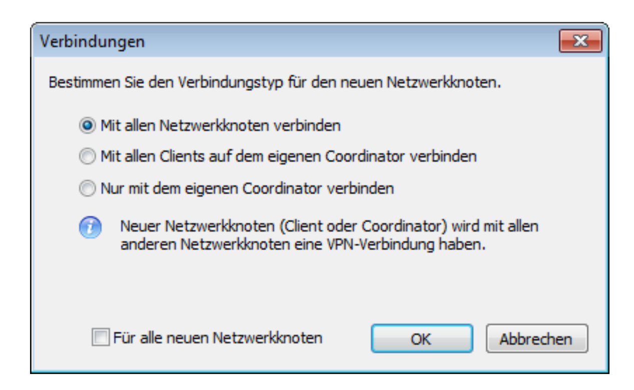


Abbildung 63. Verbindungstyp für einen neuen Netzwerkknoten wählen

- Klicken Sie auf **OK**.

In der Navigationsleiste wird der neue Netzwerkknoten angezeigt. Sein Name wird gemäß der Vorlage erstellt, die bereits beim Erstellen der Netzwerkstruktur angewendet wurde (s. Automatische Generierung der ViPNet Netzwerkstruktur auf S. 86). Bei Bedarf kann der Name des Netzwerkknotens geändert werden.

Verbindungstypen für neue Netzwerkknoten konfigurieren

Wenn Sie den standardmäßig gewählten Verbindungstyp für die neuen Netzwerkknoten ändern möchten:

1 Wählen Sie im Menü **Extras** den Eintrag **Einstellungen**.

2 Wählen Sie im Fenster **Einstellungen** in der Navigationsleiste den Bereich **Verbindungen**.

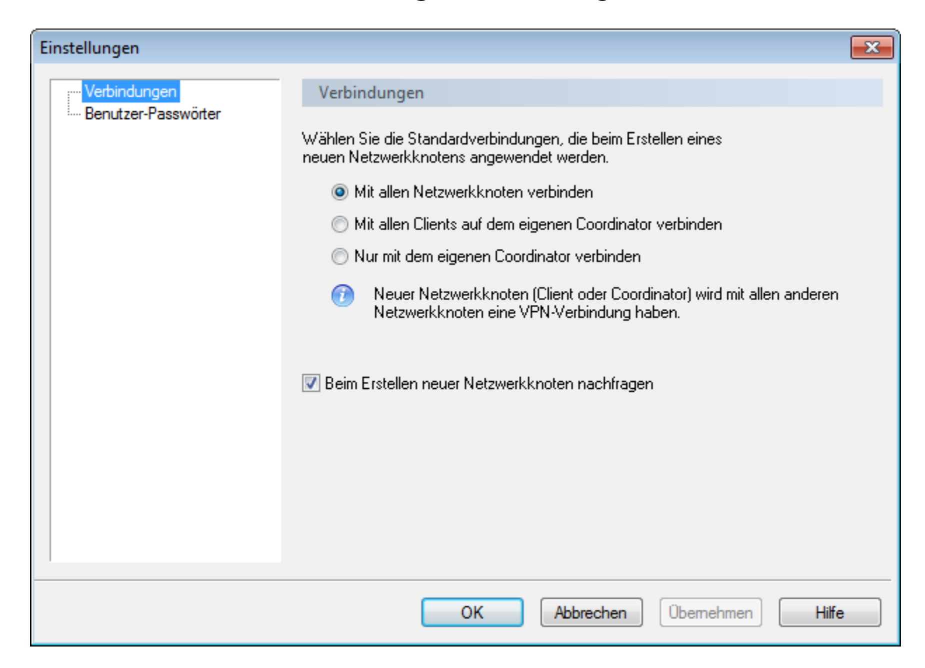


Abbildung 64. Verbindungstypen für neue Netzwerkknoten konfigurieren

3 Wählen Sie im Bereich **Verbindungen** einen der folgenden Verbindungstypen aus:

- **Mit allen Netzwerkknoten verbinden** (standardmäßig gewählt). Der geschützte Netzwerkknoten wird mit allen anderen Netzwerkknoten verbunden.
- **Mit allen Clients auf dem eigenen Coordinator verbinden**. Der Client wird mit seinem eigenen Coordinator sowie mit allen anderen Clients dieses Coordinators verbunden. Der Coordinator wird mit allen anderen Coordinatoren verbunden.
- **Nur mit dem eigenen Coordinator verbinden**. Der Client wird nur mit seinem eigenen Coordinator verbunden. Der Coordinator wird mit allen anderen Coordinatoren verbunden.

4 Damit das Fenster **Verbindungen** nicht jedes Mal beim Erstellen eines neuen Clients geöffnet wird, deaktivieren Sie das Kontrollkästchen **Beim Erstellen neuer Netzwerkknoten nachfragen** (standardmäßig deaktiviert).

5 Klicken Sie auf **OK**, um die Einstellungen zu speichern.

Client einem anderen Coordinator zuordnen

Wenn Sie den Client einem anderen Coordinator zuordnen möchten, führen Sie folgende Schritte durch:

1 Klicken Sie in der Navigationsleiste auf den betroffenen Client und ziehen ihn auf den gewünschten Coordinator.

2 Speichern Sie die Schlüssel für diesen Client in einer Datei (s. Speichern der Schlüsseldistributionen auf S. 142).

3 Installieren Sie manuell die Schlüsseldistribution (s. Installation der Schlüsseldistribution auf S. 216) auf dem Client-Knoten.

Ändern der Verbindungen zwischen den Netzwerkknoten

Führen Sie die folgenden Schritte durch, um die Verbindungen des Netzwerkknotens zu ändern:

1 Wählen Sie den gewünschten Netzwerkknoten in der Navigationsleiste aus und öffnen in der Panel-Ansicht die Registerkarte **Verbindungen**.

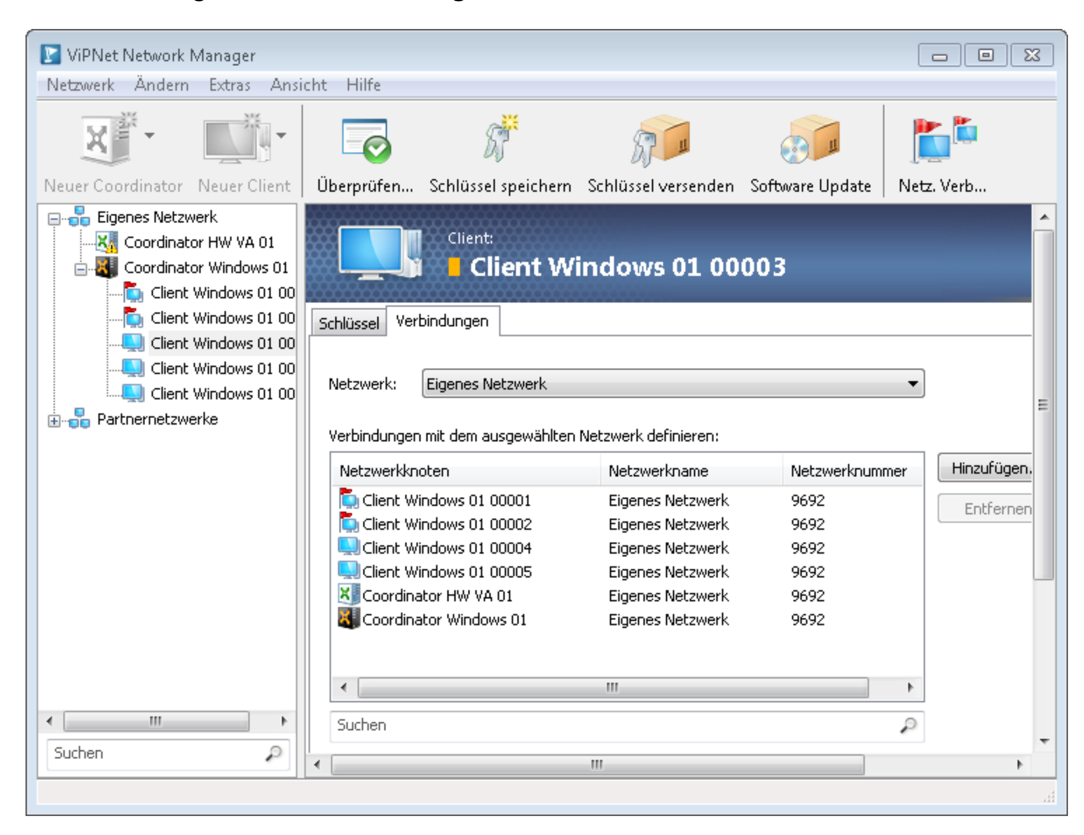


Abbildung 65. Verbindungen des Netzwerkknotens

2 Wählen Sie in der Liste **Netzwerk** einen der folgenden Punkte aus:

- **Eigenes Netzwerk**, wenn die Verbindungen zu den Knoten des eigenen Netzwerks geändert werden sollen.
- Eines der Partnernetzwerke (falls Partnernetzwerk-Verbindungen definiert wurden), um die Verbindungen mit den Netzwerkknoten dieses Netzwerks zu ändern.
- **Alle Netzwerke**, um die Verbindungen mit einem beliebigen Netzwerkknoten im eigenen Netzwerk oder in den Partnernetzwerken zu ändern.

3. Zum Hinzufügen einer Verbindung, klicken Sie auf **Hinzufügen**. Dann wählen Sie im Fenster **Verbindungen hinzufügen** einen oder mehrere Netzwerkknoten, zu denen eine Verbindung aufgebaut werden soll, und klicken auf **OK**.
4. Zum Löschen einer Verbindung zwischen zwei Netzwerkknoten, wählen Sie in der Liste **Verbindungen mit dem ausgewählten Netzwerk definieren** einen oder mehrere Netzwerkknoten aus, zu denen die Verbindung gelöscht werden soll, dann klicken auf **Löschen**.



Hinweis. Es ist nicht möglich, obligatorische Verbindungen zu löschen: das sind Verbindungen zwischen dem Coordinator und seinen Clients sowie Verbindungen zwischen dem Coordinator, dem der Client mit dem Manager-Arbeitsplatz zugeordnet ist, und anderen Coordinatoren.

Änderungen an den Verbindungen zwischen den Clients können Auswirkungen auf die Partnernetzwerk-Kommunikation haben. Deswegen sollte überprüft werden, ob ausgehende Partnernetzwerk-Informationen für irgendein Partnernetzwerk erstellt wurden. Wenn diese Daten erstellt wurden, sollten diese an den Administrator des betroffenen Partnernetzwerks weitergeleitet werden (s. Ändern von Partnernetzwerk-Verbindungen auf S. 176).

Zuweisung des Manager-Arbeitsplatzes an einen anderen Knoten

Beim erstmaligen Aufbau des Netzwerks wird in Abhängigkeit vom gewählten Standorttyp automatisch der erste Client des ersten Coordinators oder der erste Coordinator als Manager-Arbeitsplatz (Arbeitsstation des ViPNet Administrators) festgelegt. Auf dem Netzwerkknoten, der als Manager-Arbeitsplatz eingerichtet wird, sollten folgende Programme installiert sein:

- ViPNet Network Manager;
- ViPNet Client oder ViPNet Coordinator für Windows.

Bei Bedarf kann ein anderer Netzwerkknoten als Arbeitsstation des ViPNet Netzwerkadministrators festgelegt werden. Dies kann erforderlich sein, wenn zum Beispiel beim Aufbauen des ViPNet Netzwerks mit Hilfe eines Assistenten ein Client als Manager-Arbeitsplatz automatisch festgelegt wurde, obwohl es geplant war, die Arbeitsstation des Administrators auf dem Coordinator einzurichten.



Achtung! Wenn Sie früher eine Partnernetzwerkverbindung mit ViPNet VPN Netzwerke der Version niedriger als 3.0.4 eingestellt haben, dann ist es nicht möglich, der Manager-Arbeitsplatz an Coordinator zuweisen. In diesem Fall empfehlen wir, die Software ViPNet VPN in den Partnernetzwerken auf Version 3.0.4 oder höher zu aktualisieren.

Gehen Sie zum Festlegen eines Netzwerkknotens als Manager-Arbeitsplatz wie folgt vor:

1. Wählen Sie im Hauptprogrammfenster von ViPNet Network Manager in der Navigationsleiste den Netzwerkknoten aus, auf dem ein Manager-Arbeitsplatz installiert werden soll.
2. Führen Sie eine der folgenden Aktionen aus:
    - Klicken Sie mit der rechten Maustaste auf den Netzwerkknoten und wählen im Kontextmenü den Befehl **Als Manager-Arbeitsplatz festlegen**.
    - Wählen Sie im Menü **Ändern** den Befehl **Als Manager-Arbeitsplatz festlegen**.



Achtung! Ein Client mit dem Typ Client Mac OS, ThinClient, Client Android oder Client iOS IPsec sowie ein Coordinator mit dem Typ ViPNet Coordinator HW/VA kann nicht als Manager-Arbeitsplatz festgelegt werden.

3. Falls die Schlüssel für den Manager-Arbeitsplatz auf dem aktuellen Computer bereits installiert sind, klicken Sie im eingeblendeten Fenster mit dem Hinweis zu weiteren Schritten auf die Schaltfläche **Fortsetzen** und übertragen den Manager-Arbeitsplatz auf einen anderen Netzwerkknoten (s. Verlegen des Manager-Arbeitsplatzes auf einen anderen Netzwerkknoten auf S. 67).

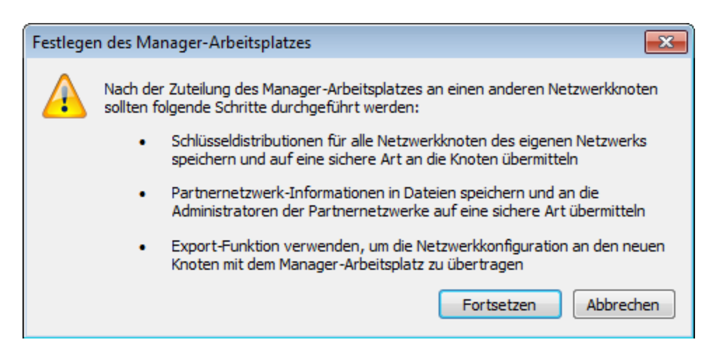


Abbildung 66. Zuweisung des Manager-Arbeitsplatzes an einen anderen Knoten



Hinweis. Wenn als Manager-Arbeitsplatz ein Client festgelegt wird, der auf einem anderen Coordinator registriert ist, dann werden automatisch obligatorische Verbindungen zwischen dem Coordinator, auf dem der neue Manager-Arbeitsplatz registriert ist, und den anderen Coordinatoren erstellt.

6

Verwaltung des ViPNet Netzwerkes

Konfiguration der Eigenschaften der Benutzerpasswörter

Zum Anzeigen oder Ändern der Eigenschaften zufälliger Passwörter:

1 Wählen Sie im Menü **Extras** den Eintrag **Einstellungen**.

2 Wählen Sie im Fenster **Einstellungen** in der Navigationsleiste den Bereich **Passwörter**.

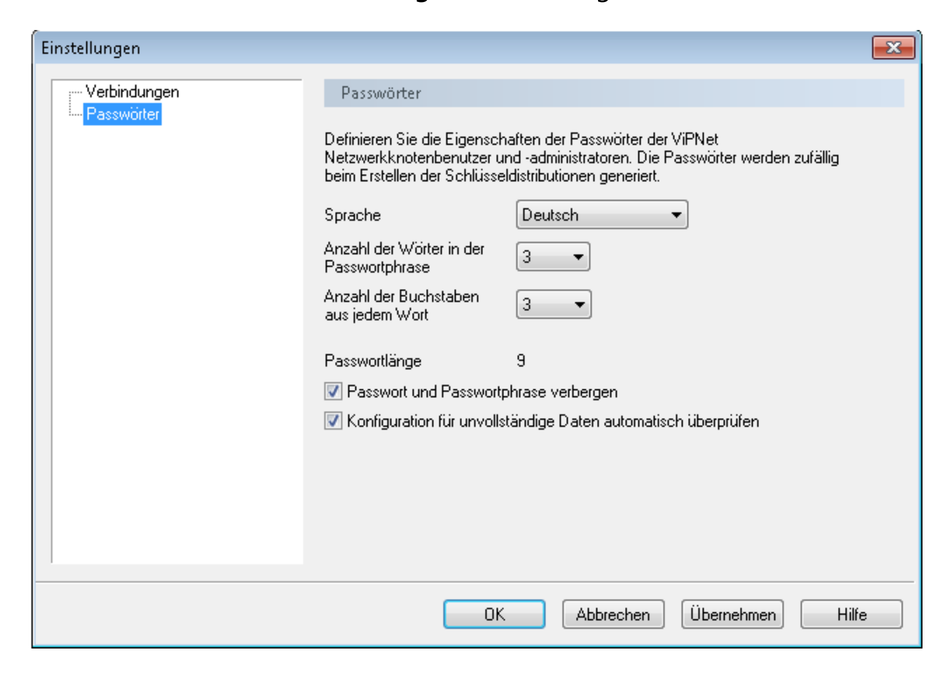


Abbildung 67. Eigenschaften der Benutzerpasswörter

3 Sie können die Eigenschaften der Zufallspasswörter mit Hilfe folgender Parameter definieren:

- **Sprache**. Wählen Sie in der Liste die Sprache aus, die für die Generierung der Passwortphrase verwendet werden soll. Folgende Sprachen sind verfügbar: Deutsch, Englisch, Französisch.
- **Anzahl der Wörter in der Passwortphrase**. Wählen Sie in der Liste die Anzahl der Wörter in der Passwortphrase aus. Bei Auswahl von 3 oder 4 Wörtern wird eine Passwortphrase generiert. Bei Auswahl von 6 oder 8 Wörtern werden 2 Passwortphrasen generiert.
- **Anzahl der Buchstaben aus jedem Wort**. Wählen Sie in der Liste die Anzahl der Anfangsbuchstaben aus jedem Wort aus (3 oder 4), die für die Zusammensetzung des Benutzerpassworts verwendet werden.
- **Passwortlänge**. In diesem Feld wird angezeigt, wie viele Buchstaben das Passwort gemäß den vorgenommenen Einstellungen enthalten wird.

4 Damit die Passwörter der Netzwerkknotenbenutzer und die Passwortphrasen in der Registerkarte **Schlüssel** in Klartext dargestellt werden, deaktivieren Sie das Kontrollkästchen **Passwort und Passwortphrase verbergen** (standardmäßig aktiviert).

5 Nachdem Sie die Einstellungen vorgenommen haben, klicken Sie auf **OK**.



Hinweis. Um das Passwort zu erhalten, sollten Sie unter Verwendung der englischen Tastaturbelegung die zuvor angegebene Anzahl der Buchstaben eines jeden Wortes der Passwortphrase ohne Leerzeichen eingeben. Beim Programmstart sollte zum Beispiel für die Passwortphrase „Fahrer fuhr toll" bei Verwendung der Standard-Passwortparameter (3 Buchstaben aus jedem Wort) und der englischen Tastaturbelegung die Zeichenfolge „fahfuhtol" eingegeben werden.

Ändern des Administrator-Passworts

Im Programm ViPNet Network Manager haben Sie die Möglichkeit, sowohl das Administratorpasswort von ViPNet Network Manager (s. ViPNet Network Manager Administratorpasswort auf S. 374) als auch das Passwort des Netzwerkknotenadministrators (s. Netzwerkknotenadministrator-Passwort auf S. 371) des gesamten ViPNet Netzwerks zu ändern.

Führen Sie die folgenden Schritte aus, um das Administratorpasswort des Programms ViPNet Network Manager oder das Passwort des Netzwerkknotenadministrators zu ändern:

1 Klicken Sie im Menü **Extras** auf den Eintrag **Passwort ändern** und wählen dann eine der folgenden Optionen aus:

   - **Passwort des Administrators von ViPNet Network Manager**,
   - **Passwort des Netzwerkknoten-Administrators**.

2 Wenn Sie das Passwort des Administrators von ViPNet Network Manager ändern möchten, dann geben zunächst im eingeblendeten Fenster das aktuelle Passwort für die Anmeldung im Programm ViPNet Network Manager ein und klicken dann auf **OK**.

3 Wählen Sie im eingeblendeten Fenster mit den Passwortoptionen in der Liste **Passworttyp** einen der folgenden Einträge aus:

   - **Zufälliges**: das Passwort wird zufällig auf Basis einer Passwortphrase gebildet.

     Bei Auswahl eines zufälligen Passworts werden in den entsprechenden Feldern das vorgeschlagene Passwort und die Passwortphrase angezeigt.

     - Klicken Sie auf **OK**, um das vorgeschlagene Passwort zu akzeptieren.
     - Klicken Sie auf **Neues**, um ein anderes Passwort zu generieren.



Tipp. Klicken Sie auf **Eigenschaften**, um die Parameter für das Erzeugen zufälliger Passwörter zu ändern. Es wird das Fenster **Eigenschaften des zufälligen Passworts** (s. Konfiguration der Eigenschaften der Benutzerpasswörter auf S. 139) eingeblendet.

   - **Benutzerdefiniertes**: das Passwort wird vom Benutzer selbständig vergeben.

     Bei Auswahl eines benutzerdefinierten Passworts:

     - Geben Sie in den entsprechenden Feldern das gewünschte Passwort ein und bestätigen es.
     - Klicken Sie auf **OK**, um das Passwort zu speichern.

4 Wenn Sie das Passwort des Netzwerkknotenadministrators geändert haben, dann erstellen anschließend die Updates der Schlüssel und versenden diese an die Clients und Coordinatoren des eigenen ViPNet Netzwerks (s. Versenden der Schlüssel-Updates auf S. 145).

   Wenn Sie das Administratorpasswort des Programms ViPNet Network Manager geändert haben, dann sind keine weiteren Schritte nötig.

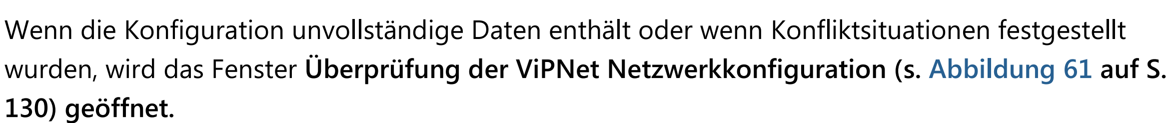
Speichern der Schlüsseldistributionen

Die Schlüsseldistributionen für die ViPNet Netzwerkknoten sollten in Dateien `*.dst` (s. Schlüsseldistribution auf S. 373) gespeichert werden, um sie später für die Installation oder für die Aktualisierung der Adresslisten und Schlüssel auf den entsprechenden Knoten zu benutzen (s. Installation der Schlüsseldistribution auf S. 216). Dies kann in folgenden Fällen erforderlich werden:

- Es wurde eine neue Struktur des ViPNet Netzwerks (s. Automatische Generierung der ViPNet Netzwerkstruktur auf S. 86) angelegt. Nun müssen auf den Netzwerkknoten Adresslisten und Schlüssel installiert werden.
- An der Struktur des ViPNet Netzwerks wurden Änderungen (s. Ändern der ViPNet Netzwerkstruktur auf S. 89) vorgenommen, das Versenden der Schlüsselupdates über verschlüsselte Verbindungskanäle ist aber aus irgendwelchen Gründen nicht möglich.

Führen Sie die folgenden Aktionen durch, um die Schlüsseldistributionen zu speichern:

1 Führen Sie einen der folgenden Schritte durch:

   - Wählen Sie im Menü **Extras** den Eintrag **Schlüssel** und klicken dann auf **Schlüsseldistributionen speichern**.
   - Klicken Sie auf der Symbolleiste auf die Schaltfläche **Schlüssel speichern**  .

   Wenn die Konfiguration unvollständige Daten enthält oder wenn Konfliktsituationen festgestellt wurden, wird das Fenster **Überprüfung der ViPNet Netzwerkkonfiguration (s. Abbildung 61 auf S. 130) geöffnet.**

2 Wenn in der Netzwerkkonfiguration Konfliktsituationen oder unvollständige Daten vorhanden sind, sollten diese zunächst behoben werden (s. Erkennen von Konfliktsituationen und unvollständigen Daten in der ViPNet Netzwerkkonfiguration auf S. 128), anderenfalls wird das Erstellen der Schlüsseldistributionen nicht möglich sein. Wenn nur unvollständige Daten festgestellt wurden, können Sie auf die Schaltfläche **Überspringen** klicken und das Erstellen der Schlüsseldistributionen fortsetzen. Nach der Installation der ViPNet Software auf den Netzwerkknoten werden jedoch manuelle Einstellungen unmittelbar auf jedem Netzwerkknoten erforderlich sein.

3 Aktivieren Sie im Fenster **Speichern der Schlüsseldistributionen** die Kontrollkästchen neben den Knoten, für welche die Schlüssel generiert werden sollen. Standardmäßig sind die Kontrollkästchen bei allen Knoten aktiviert, für die noch keine Schlüssel erstellt wurden.

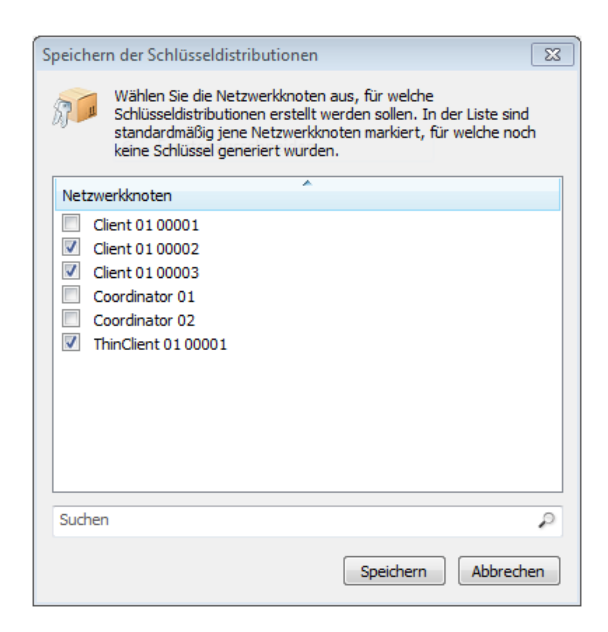


Abbildung 68. Auswahl der Knoten zum Speichern der Schlüssel

4 Geben Sie im Fenster **Ordner auswählen** den Ordner an, in welchem die Dateien der Schlüsseldistributionen gespeichert werden sollen.

5 Wenn die Erstellung der Schlüssel abgeschlossen ist, wird im Explorer-Fenster von Windows der Ordner angezeigt, in welchem die zuvor erstellten Netzwerkknotenschlüssel sowie die Benutzer- und Administratorpasswörter von ViPNet gespeichert wurden.

Die Dateien der Schlüsseldistributionen besitzen die Erweiterung `.dst` und werden in Ordnern abgelegt, deren Namen den Netzwerkknotennamen entsprechen. Benutzerpasswörter werden in der Datei `ViPNet.txt` in Form einer Liste abgelegt. Das gemeinsame Administratorpasswort für alle ViPNet Netzwerkknoten wird im Bereich **Eigenes Netzwerk** in der Registerkarte **Passwörter** angezeigt.

Wenn in Ihrem Netzwerk die Coordinatoren ViPNet Coordinator HW/VA verwendet werden, werden es auch die folgende Konfigurationsdateien erstellt, die es ermöglichen, auf dem Coordinator die Einstellungen automatisch übernehmen, die früher im ViPNet Network Manager eingegeben wurden:

- Im Ordner der Netzwerkknotenschlüssel der Coordinatoren ViPNet Coordinator HW/VA werden die Dateien `hwinit_set.xml` erstellt. Diese Dateien dienen der automatischen Installation der Schlüssel auf einen bestimmten Coordinator.
- Im allgemeinen Ordner der Schlüssel wird die Datei `hwinit_reset.xml` erstellt. Diese Datei dient der automatischen Wiederherstellung von Standardeinstellungen in der Software ViPNet Coordinator HW/VA (und kann auf beliebigen Coordinatoren ViPNet Coordinator HW/VA verwendet werden).

6 Kopieren Sie die Schlüssel und die Benutzerkennwörter auf einen Wechseldatenträger (z. B. CD oder USB-Stick). Diese Kopien der Schlüsseldistributionen können Sie für die Installation oder Aktualisierung der Adresslisten und Schlüssel auf den Netzwerkknoten verwenden (s. Installation der Schlüsseldistribution auf S. 216).

In Abhängigkeit davon, welche Art von Einstellungen auf dem Coordinator ViPNet Coordinator HW/VA vorgenommen werden soll, kopieren Sie eine der Konfigurationsdateien auf den USB-

Datenträger. Wenn Netzwerkknotenschlüssel auf den Coordinator installiert werden sollen, kopieren Sie zusätzlich die Datei mit der Erweiterung `.dst`. Übergeben Sie dann den USB-Datenträger mit der benötigten Konfigurationsdatei dem Administrator des Coordinators.

Versenden der Schlüssel-Updates

Wenn an der Konfiguration des ViPNet Netzwerks Änderungen vorgenommen wurden, dann sollten aktualisierte Schlüsseldistributionen an alle Netzwerkknoten versendet werden, die von den Änderungen betroffen sind. Wenn die Schlüsseldistributionen werden zum ersten Mal auf Netzwerkknoten installiert, dann führen Sie die Installation manuell durch (mit Hilfe der Dateien `*.dst`), indem Sie einen externen Datenträger benutzen (s. Installation der Schlüsseldistribution auf S. 216).

Stellen Sie vor dem Versenden der Schlüsselupdates sicher, dass auf dem Manager-Arbeitsplatz das Programm ViPNet Client oder ViPNet Coordinator gestartet ist (dieses Programm startet das MFTP-Modul, das den Versand der Schlüssel durchführt).

Gehen Sie wie folgt vor, um die Schlüsselupdates an die ViPNet Netzwerkknoten zu versenden:

1 Führen Sie einen der folgenden Schritte durch:

- Klicken Sie auf **Schlüsseldistributionen versenden** auf der Symbolleiste.
- Wählen Sie im Menü **Extras** den Eintrag **Schlüssel** und klicken dann auf **Schlüsseldistributionen versenden**.

2 Wenn die Software ViPNet auf dem Manager-Arbeitsplatz nicht richtig konfiguriert ist, wird die Meldung mit der Problembeschreibung und möglichen Lösung geöffnet. Versuchen Sie das Problem zu beheben und die Updates erneut zu senden.

3 Wenn neue Netzwerkknoten zum ViPNet Netzwerk hinzugefügt wurden, sollte das Update auf der Arbeitsstation des Administrators vor dem Versand von Schlüsselupdates an die Netzwerkknoten angenommen werden. Wenn die Schlüsselupdates noch nicht auf dem Manager-Arbeitsplatz übernommen wurden, dann wird vom Programm eine Warnmeldung angezeigt.

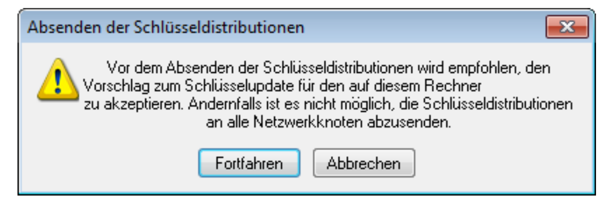


Abbildung 69. Auf dem Manager-Arbeitsplatz sollte das Schlüsselupdate akzeptiert werden

Klicken Sie auf **Fortfahren**, um das Schlüsselupdate auf dem Manager-Arbeitsplatz zu installieren.

4 Stellen Sie sicher, dass im Fenster **Versenden der Schlüsseldistributionen** die Kontrollkästchen neben den Netzwerkknoten, an welche die Schlüsselupdates gesendet werden sollen, aktiviert sind. Standardmäßig sind alle Kontrollkästchen aktiviert.



Hinweis. Es können keine Schlüsselupdates an Clients versendet werden, auf denen die Software ViPNet Client for Mac OS X installiert ist. Solche Clients werden im Fenster **Versenden der Schlüsseldistributionen** nicht angezeigt. Leiten Sie die Schlüsseldistributionen an die Benutzer dieser Knoten manuell weiter.

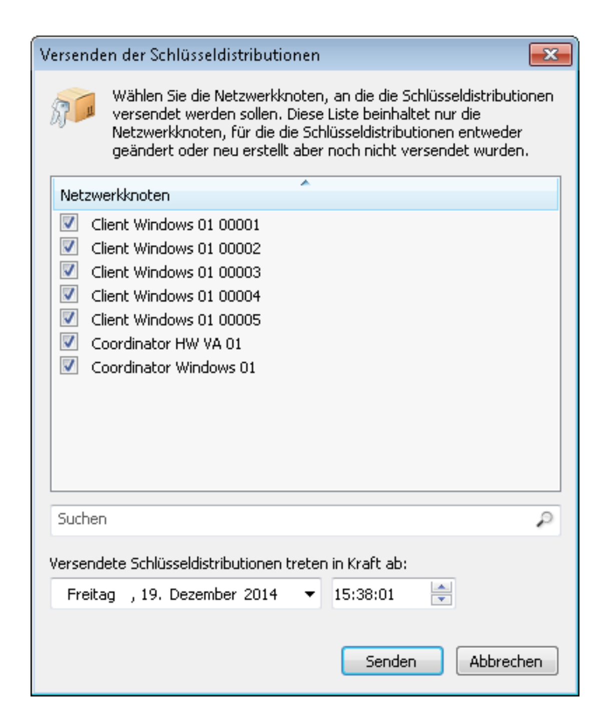


Abbildung 70. Versenden der Schlüsseldistributionen

5 Um die Auswahl einzuschränken, geben Sie im Suchfeld einige Symbole ein, die in den Netzwerkknotennamen vorkommen können. Es können auch Ziffern eingegeben werden, um die Netzwerkknoten nach dem Erstell- oder Änderungsdatum der Schlüssel zu filtern.

6 Um die Zeit einzugeben, ab der die Schlüsseldistributionen in Kraft treten, verwenden Sie das Feld **Versendete Schlüsseldistributionen treten in Kraft ab**, um den Zeitpunkt zu definieren, zu dem die Updates in Kraft treten sollen. Standardmäßig werden das aktuelle Datum und die Uhrzeit angezeigt.

7 Klicken Sie auf **Senden**. Das MFTP-Transportmodul (s. ViPNet MFTP auf S. 30) wird gestartet und der Versand der Schlüsseldistributionen beginnt. Beim Auftreten von Problemen zeigt das Programm entsprechende Fehlermeldungen an. Falls der Versand erfolgreich durchgeführt werden konnte, wird ebenfalls eine Meldung angezeigt.

Versand und Speicherung der Netzwerkknotenschlüssel

Wenn die Änderungen der Netzwerkkonfiguration nur einen Netzwerkknoten betreffen (z. B. das Benutzerpasswort wurde geändert), ist es einfacher, die Schlüsseldistribution nur für diesen Netzwerkknoten zu aktualisieren.

Neue Schlüsselupdates können auf zwei Arten an die Netzwerkknoten weitergeleitet werden: entweder kann das Update direkt über das geschützte ViPNet Netzwerk übermittelt werden oder es kann eine Datei `*.dst` erstellt werden, um mit ihrer Hilfe die Adresslisten und Schlüssel manuell zu aktualisieren.

Führen Sie die folgenden Aktionen durch, um das Schlüsselupdate für einen bestimmten Netzwerkknoten zu erstellen:

1 Wählen Sie in der Navigationsleiste den Netzwerkknoten aus, für den die Schlüsseldistribution erstellt werden soll.

2 Öffnen Sie in der Panel-Ansicht die Registerkarte **Schlüssel**.

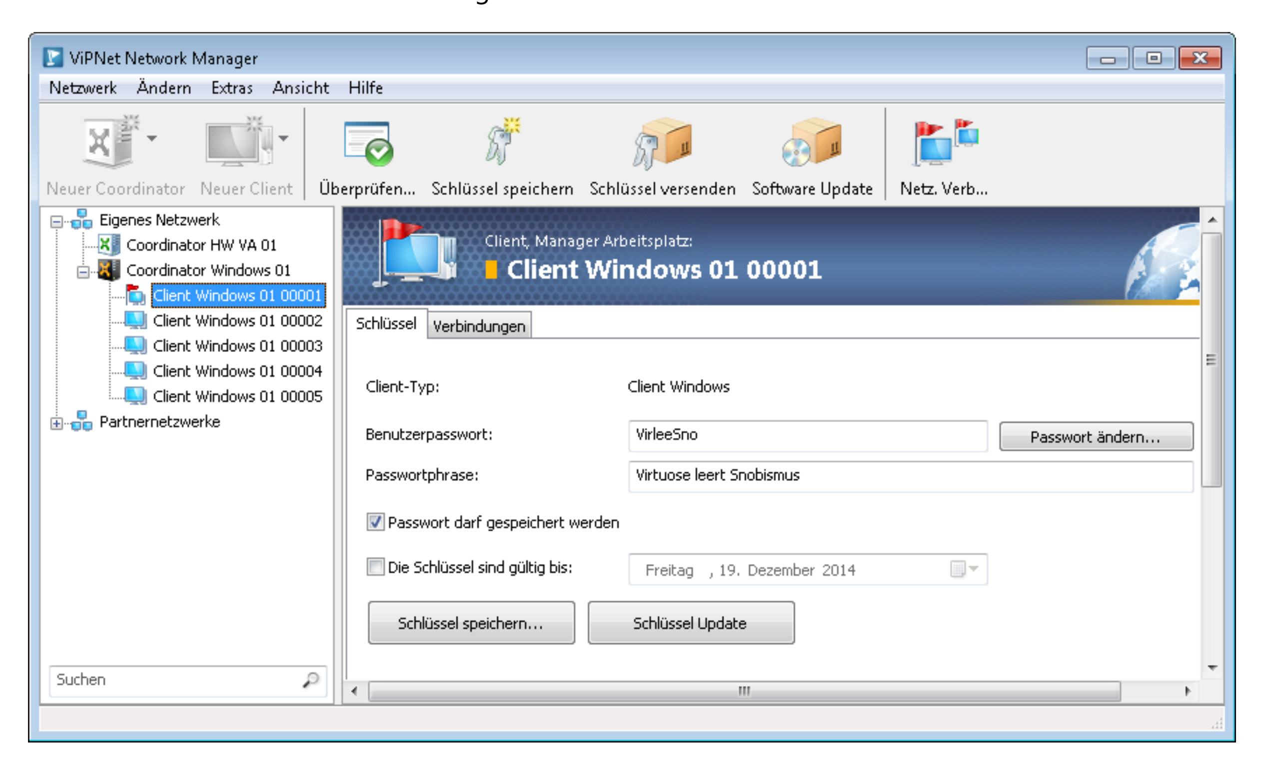


Abbildung 71. Schlüsseldistribution für einen bestimmten Netzwerkknoten erstellen

3 Begrenzen Sie, wenn nötig, die Gültigkeitsdauer der Schlüssel. Dazu:

- Aktivieren Sie das Kontrollkästchen **Die Schlüssel sind gültig bis**.
- Geben Sie mit Hilfe des Kalenderelements das Datum an, das die Gültigkeitsdauer der Schlüssel begrenzt. Nach Ablauf der Gültigkeit der Schlüssel wird der Benutzer nicht mehr in der Lage sein, ViPNet Software auf dem gegebenen Netzwerkknoten auszuführen.

Standardmäßig ist die Gültigkeitsdauer der Netzwerkknotenschlüssel unbegrenzt.



Hinweis. Es kann keine Gültigkeitsdauer der Netzwerkknotenschlüssel definiert werden, die den Gültigkeitszeitraum der Lizenz überschreitet (falls die ViPNet VPN-Lizenz zeitlich begrenzt ist). Wählen Sie in Menü **Hilfe** den Eintrag **Über**, um weitere Informationen zur Gültigkeitsdauer der Lizenz zu erhalten.

4 Falls auf dem gegebenen Netzwerkknoten früher bereits ViPNet Adresslisten und Schlüssel installiert wurden und wenn zu diesem Knoten eine verschlüsselte Verbindung aufgebaut werden kann, dann führen Sie folgende Aktionen aus, um eine Schlüsseldistribution an diesen Knoten zu versenden:

4.1 Klicken Sie auf **Schlüssel Update**. Es wird das Fenster **Versenden der Schlüsseldistributionen** geöffnet.

4.2 Wenn nötig, geben Sie den Zeitpunkt an, zu dem die Aktualisierungen wirksam werden sollen. Klicken Sie dann auf **Senden** (s. Versenden der Schlüssel-Updates auf S. 145).

5 Wenn aus irgendwelchen Gründen das Versenden von Schlüsseln über das ViPNet Netzwerk nicht möglich ist, dann führen Sie folgende Aktionen aus, um die Schlüssel in einer Datei zu speichern:

5.1 Klicken Sie auf **Schlüssel speichern**.

5.2 Geben Sie im Fenster **Ordner auswählen** den Ordner an, in welchem die Datei der Schlüsseldistribution abgelegt werden soll.

Es wird mit dem Erstellen der Schlüsseldistribution (s. Speichern der Schlüsseldistributionen auf S. 142) begonnen. Nach Abschluss des Vorgangs wird im Windows-Explorer der Ordner geöffnet, der die Schlüsseldistribution für den gewählten Netzwerkknoten sowie das Benutzer- und das Administratorpasswort enthält.

5.3 Übertragen Sie die erstellte Schlüsseldistributionsdatei auf den entsprechenden Netzwerkknoten und aktualisieren mit Hilfe dieser Datei die Adresslisten und Schlüssel des Knotens (s. Installation der Schlüsseldistribution auf S. 216).

Versenden von ViPNet Softwareupdates



Achtung! Ein Update der ViPNet Software kann nur auf denjenigen Netzwerkknoten durchgeführt werden, auf denen ViPNet Software der Version 2.8.12 oder höher installiert ist, und deren Benutzer über Administratorrechte im Betriebssystem Windows verfügen. Wenn auf dem Netzwerkknoten eine frühere Version der Software installiert ist oder wenn der Benutzer nicht über Administratorrechte auf dem Knoten verfügt, dann kann ein Update nicht durchgeführt werden. Dabei bleibt die installierte ViPNet Software voll funktionstüchtig, es können jedoch Probleme beim Hinzufügen oder Löschen einzelner Komponenten der Software auftreten.

ViPNet Network Manager ermöglicht es dem Administrator, die Software ViPNet Client, ViPNet Coordinator und ViPNet Coordinator HW/VA auf den ViPNet Netzwerkknoten remote zu aktualisieren.

Das Software-Update wird in Form von Dateien im LZH-Format an die Netzwerkknoten versendet. Wenden Sie sich an die Infotecs GmbH, wenn Sie Dateien mit Software-Updates anfordern möchten. Nachdem Sie die Software-Updates erhalten haben, legen Sie diese in einem Ordner (ohne Unterordner) ab.



Hinweis. Der Versand von Softwareupdates an Clients, auf denen die Software ViPNet Client for Mac OS X installiert ist, soll manuell durchgeführt werden.

Beachten Sie vor dem Versenden von ViPNet Software-Updates die folgenden Hinweise:

- Beachten Sie die Sprachversion des ViPNet Software-Updates. Die Sprache des Updates sollte mit der Sprache der installierten Software übereinstimmen.
- Beim Versenden von Softwareupdates sollte das Kontrollkästchen **Rechner nach dem Software-Update neu starten** aktiviert werden. Wenn das Update an Clients versendet wird, kann dieses Kontrollkästchen deaktiviert bleiben. Für Coordinatoren, auf die der Zugang eingeschränkt oder unerwünscht ist, sollte das Kontrollkästchen jedoch aktiviert werden.
- Bennen Sie die LZH-Dateien gemäß wie in der unten angeführten Tabelle um (wenn Dateinamen nicht übereinstimmen).

Tabelle 9. Namen der Aktualisierungsdateien abhängig vom Knotentyp

Knotentyp	Name der Aktualisierungsdatei
Client Windows	`driv_fsa.lzh`
Client Android	`driv-android-*.*.*-*.lzh`
ThinClient	`thinclient_vipnet_driv_*.*.*-*.lzh`

Knotentyp	Name der Aktualisierungsdatei
Coordinator Windows	driv_csa.lzh
Coordinator HW100	hw100_driv_*.*-*.lzh
Coordinator HW1000	hw1000_driv_*.*-*.lzh
Coordinator HW2000	hw2000_driv_*.*-*.lzh
Coordinator VA100	coordinatorhw_vipnet_driv_*.*-*.lzh
Coordinator VA1000	coordinatorhw_vipnet_driv_*.*-*.lzh
Coordinator VA2000	coordinatorhw_vipnet_driv_*.*-*.lzh

Zum Versenden von Softwareupdates an die ViPNet Netzwerkknoten:

1 Führen Sie einen der folgenden Schritte durch:

  - Klicken Sie auf **Software-Update** auf der Symbolleiste.
  - Wählen Sie im Menü **Extras** den Befehl **ViPNet Software Update**.

  Wenn die ViPNet Software auf dem Manager-Arbeitsplatz nicht richtig konfiguriert ist, dann werden vom Programm eine Fehlermeldung und ein Vorschlag zur Lösung des Problems angezeigt. Beheben Sie das Problem und versuchen, das Update erneut zu versenden.

2 Wenn die ViPNet Software auf dem Manager-Arbeitsplatz richtig konfiguriert ist, wird nun die erste Seite des **ViPNet Software Update** Assistenten geöffnet. Klicken Sie auf **Weiter**.

3 Klicken Sie auf der Seite **Ordner mit Software-Update** auf die Schaltfläche **Durchsuchen** und wählen den Ordner aus, in dem die Dateien mit dem Software-Update abgespeichert sind.

  Nachdem Sie den Ordner mit den Update-Dateien ausgewählt haben, klicken Sie auf **Weiter**.

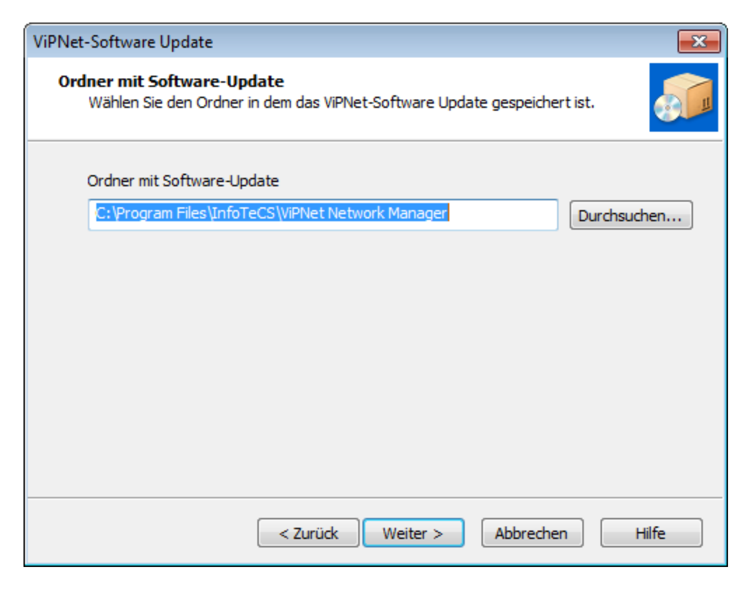


Abbildung 72. Auswahl des Ordners mit Software-Update

4 Deaktivieren Sie auf der Seite Fenster **Software-Update auf den Netzwerkknoten** die Kontrollkästchen neben den Netzwerkknoten, an die keine Updates gesendet werden sollen. Um die

Kontrollkästchen für alle Netzwerkknoten zu aktivieren, klicken Sie auf **Alle auswählen**. Um alle Kontrollkästchen zu deaktivieren, klicken Sie auf **Alle abwählen**.



Hinweis. Um die Auswahl einzuschränken, geben Sie im Feld Finden einige Symbole ein, die in den Netzwerkknotennamen vorkommen können.

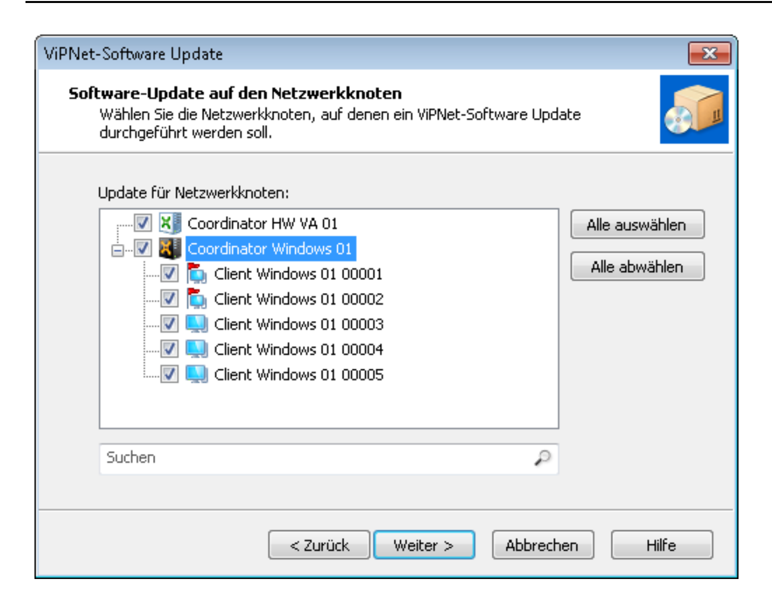


Abbildung 73. Netzwerkknoten für das Update auswählen

Wenn bestimmte Netzwerkknoten nicht ausgewählt werden können (das Kontrollkästchen ist inaktiv), dann ist das ein Hinweis darauf, dass die Schlüsseldistribution auf dem Manager-Arbeitsplatz nicht aktualisiert wurde. Klicken Sie in diesem Fall auf **Abbrechen**, erstellen Sie eine neue Schlüsseldistribution für den Manager-Arbeitsplatz (s. Speichern der Schlüsseldistributionen auf S. 142) und nehmen dieses Schlüsselupdate im Programm ViPNet Client oder ViPNet Coordinator auf dem Manager-Arbeitsplatz an.

5 Klicken Sie auf **Weiter**, um fortzufahren.

6 Ändern Sie auf der Seite **Datum des Inkrafttretens** bei Bedarf das Datum und die Zeit des Inkrafttretens der Updates. Standardmäßig ist die aktuelle Zeit und das aktuelle Datum eingestellt.

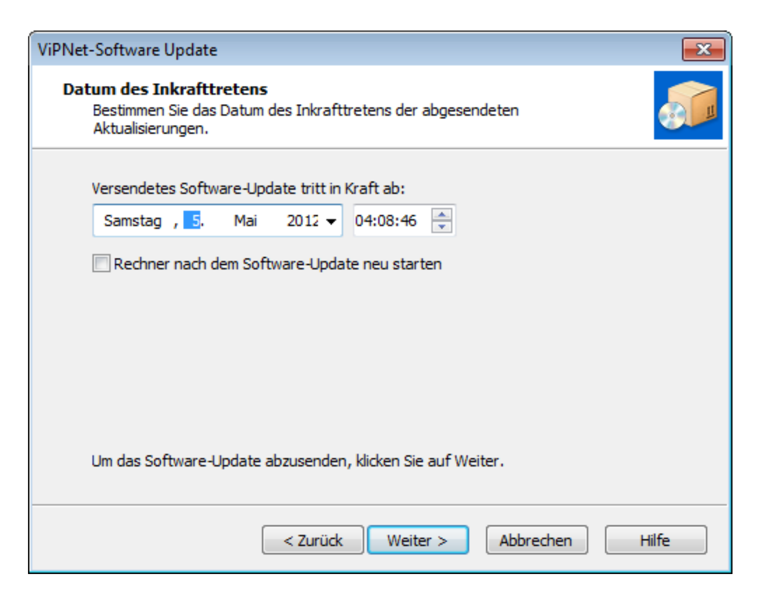


Abbildung 74. Datum des Inkrafttretens der Updates angeben

7 Wenn nach dem Durchführen der Updates die Netzwerkknoten automatisch neu gestartet werden sollen, aktivieren Sie das Kontrollkästchen **Rechner nach dem Software-Update neu starten**. Dieses Kontrollkästchen sollte aktiviert werden, wenn Updates auf Coordinatoren durchgeführt werden, auf denen keine Benutzer arbeiten.

Wenn die Benutzer ihre Computer manuell neu starten sollen, lassen Sie das Kontrollkästchen **Rechner nach dem Software-Update neu starten** deaktiviert. Nach dem Aktualisieren werden auf den Netzwerkknoten Meldungen eingeblendet, dass der Computer neu gestartet werden soll.

8 Klicken Sie auf **Weiter**. Das MFTP-Modul wird gestartet und die Updates werden versendet. Beim Auftreten von Problemen zeigt das Programm entsprechende Fehlermeldungen an. Falls der Versand erfolgreich durchgeführt werden konnte, wird ebenfalls eine Meldung angezeigt.

9 Klicken Sie auf **Fertig**, um die Arbeit mit dem Assistenten zu beenden.

Erstellen und Wiederherstellen von Sicherungskopien der ViPNet Network Manager-Konfiguration

Das Programm ViPNet Network Manager ermöglicht es, durch die Verwendung von Sicherungskopien, die entweder automatisch vom Programm oder manuell vom ViPNet Network Manager-Administrator erstellt wurden, zu früheren ViPNet Netzwerkkonfigurationen und Einstellungen zurückzukehren.

ViPNet Network Manager erstellt in den folgenden Fällen automatisch (ohne Benutzerbeteiligung) eine Sicherungskopie der aktuellen ViPNet Netzwerkkonfiguration:

- beim Schließen des Programms, wenn die Netzwerkkonfiguration oder irgendwelche Einstellungen geändert wurden;
- beim Wiederherstellen der ViPNet Netzwerkkonfiguration durch eine Sicherungskopie;
- beim Löschen der ViPNet Netzwerkstruktur;
- beim erneuten Erstellen des ViPNet Netzwerkes.

Neben der Konfiguration und den Einstellungen des ViPNet Netzwerks werden in der Sicherungskopie die aktuellen Einstellungen des Programms ViPNet Network Manager gespeichert.

Die Sicherungskopien der Konfiguration werden im Ordner `C:\ProgramData\InfoTeCS\ViPNet Manager\Restore` gespeichert.

Sicherungskopien der ViPNet Network Manager-Konfiguration sollten erstellt werden, um aktuelle Anwendungs- und ViPNet Netzwerkparameter zu sichern, damit diese Parameter zu einem späteren Zeitpunkt bei Bedarf wiederhergestellt werden können. Zum Beispiel kann eine Sicherungskopie der Konfiguration vor Durchführung wesentlicher Änderungen an der ViPNet Netzwerkstruktur angelegt werden.

Wenn ViPNet Network Manager-Einstellungen und Daten über die ViPNet Netzwerkstruktur auf einen anderen Computer übertragen werden sollen, dann nutzen Sie die Export- und Importfunktion der Konfiguration (s. Export und Import von ViPNet Network Manager-Konfigurationen auf S. 160).

Sicherungskopie der aktuellen Konfiguration erstellen



Hinweis. Wenn der Speicherplatz auf der Festplatte für die Erstellung der Sicherungskopie nicht ausreichend ist, erscheint eine Fehlermeldung. Stellen Sie ausreichend freien Speicherplatz zur Verfügung.

Zum Erstellen einer Sicherungskopie der aktuellen Konfiguration:

1 Wählen Sie im Programmfenster von ViPNet Network Manager im Menü **Extras** den Eintrag **Sicherungskopien der Konfiguration**. Der Assistent **Wiederherstellen der ViPNet Network Manager Konfiguration** wird gestartet.

2 Aktivieren Sie auf der Seite **Wiederherstellung der ViPNet Network Manager Konfiguration** das Kontrollkästchen **Sicherungskopie der aktuellen Konfiguration erstellen** und klicken auf **Weiter**.



Abbildung 75. Assistent „Wiederherstellen der ViPNet Network Manager Konfiguration"

3 Geben Sie auf der Seite **Erstellen der Sicherungskopie** im Feld **Kommentar** eine Beschreibung der Konfiguration ein. Dies ist nicht obligatorisch, wird aber helfen, die gewünschte Sicherungskopie in der Liste zu finden. Der Kommentar darf maximal 200 Zeichen lang sein.

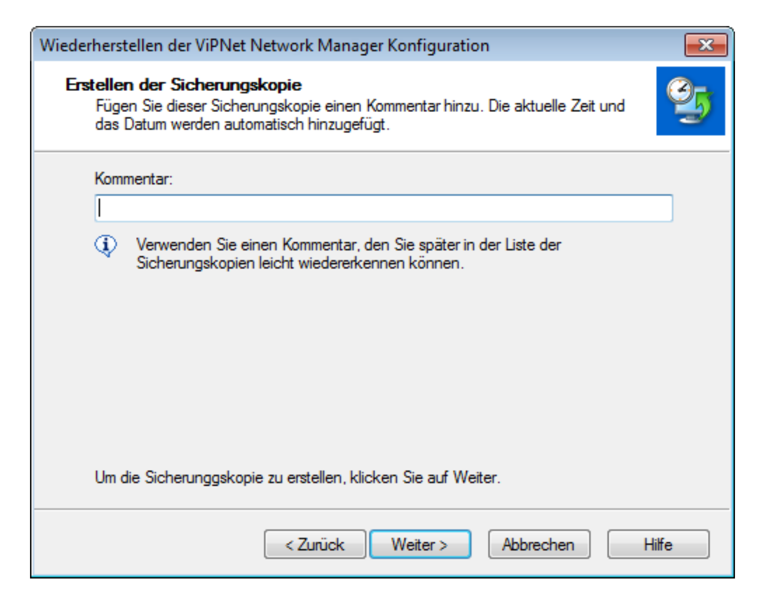


Abbildung 76. Erstellung der Sicherungskopie

4 Klicken Sie auf **Weiter**. Die Sicherungskopie der Konfiguration wird nun erstellt.

Die erstellte Sicherungskopie wird im Unterordner `\Restore` des Installationsordners des Programms gespeichert.

5 Klicken Sie auf der Seite **Abschluss der Erstellung der Sicherungskopie** auf **Fertig**, um den Assistenten abzuschließen.

6 Wenn Sie die Arbeit mit Sicherungskopien fortsetzen möchten, klicken Sie auf **Zum Anfang**.

Wiederherstellen der Konfiguration

Führen Sie die folgenden Schritte aus, um eine Konfiguration von ViPNet Network Manager aus einer zuvor gespeicherten Sicherungskopie wiederherzustellen:

1 Wählen Sie im Menü **Extras** den Befehl **Sicherungskopien der Konfiguration**. Der Assistent **Wiederherstellen der ViPNet Network Manager Konfiguration** wird gestartet.

2 Aktivieren Sie auf der Seite **Wiederherstellung der ViPNet Network Manager Konfiguration** die Option **ViPNet Network Manager Konfiguration wiederherstellen** und klicken anschließend auf **Weiter**.

3 Auf der Seite **Auswahl der Sicherungskopie** wird eine Liste der gespeicherten Sicherungskopien angezeigt.

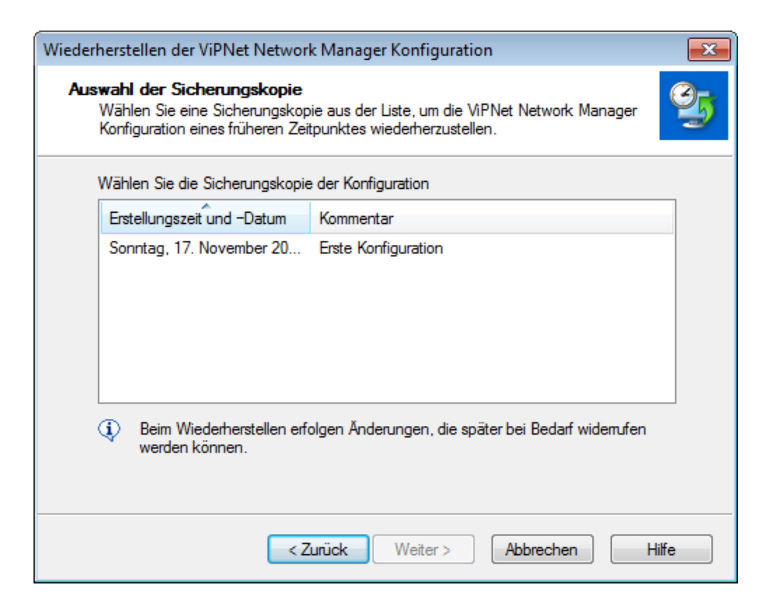


Abbildung 77. Auswahl der Sicherungskopie

Die Sicherungskopien, die automatisch erstellt wurden, können folgende Kommentare haben:

- Erstellt beim Beenden des Programms.
- Erstellt beim Wiederherstellen der Konfiguration.
- Erstellt beim Erstellen des Netzwerks.
- Erstellt beim Löschen des Netzwerks.

Die Sicherungskopien werden automatisch nach Erstellungsdatum oder nach Kommentaren sortiert. Um die Reihenfolge der Sortierung zu ändern, klicken Sie auf die Überschrift der Spalte **Erstellungszeit und Datum** oder **Kommentar**.

Wählen Sie die Sicherungskopie, die Sie für das Wiederherstellen verwenden möchten, und klicken auf **Weiter**.

4 Wenn nach dem Erstellen der Sicherungskopie das Passwort für ViPNet Network Manager geändert wurde, geben Sie im Fenster **Passwort** das Passwort, das zum Zeitpunkt der Erstellung der Sicherungskopie gültig war, ein und klicken auf **Weiter**.

Die Wiederherstellung der Konfiguration wird gestartet.

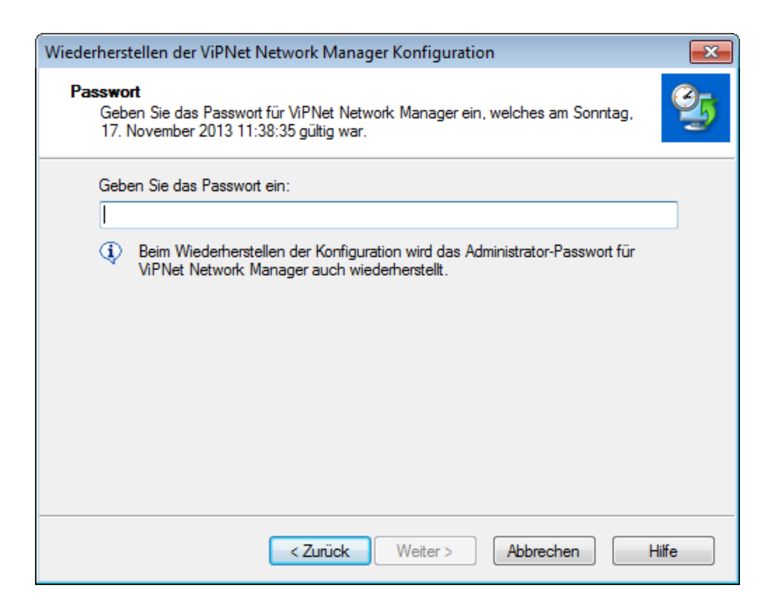


Abbildung 78. Eingabe des Passwortes für ViPNet Network Manager, das bei der Erstellung der Sicherungskopie gültig war

5 Wenn Sie die Arbeit mit Assistent beenden möchten, klicken Sie auf der Seite **Abschluss der Wiederherstellung der ViPNet Network Manager Konfiguration** auf die Schaltfläche **Schließen**.



Hinweis. Die letzte Wiederherstellung kann immer rückgängig gemacht werden. Außerdem kann die Wiederherstellung aus einer anderen Sicherungskopie eingeleitet werden, indem Sie zur ersten Seite des Assistenten zurückkehren. Wenn der Assistent bereits beendet wurde, starten Sie ihn neu.

Liste von Sicherungskopien der Konfiguration editieren

Die Liste der Sicherungskopien kann bearbeitet werden: die Kopien können gelöscht und die Kommentare geändert werden.

Zum Bearbeiten der Liste der Sicherungskopien:

1 Wählen Sie im Programmfenster von ViPNet Network Manager im Menü **Extras** den Befehl **Sicherungskopien der Konfiguration**. Der Assistent **Wiederherstellen der ViPNet Network Manager Konfiguration** wird gestartet.

2 Wählen Sie auf der Seite **Wiederherstellung der ViPNet Network Manager Konfiguration** die Option **Die Liste der Sicherungskopien ändern** und klicken anschließend auf **Weiter**.

3 Wählen Sie auf der Seite **Ändern der Liste der Sicherungskopien** die Sicherungskopie aus, die Sie bearbeiten wollen. Wenn Sie den Kommentar zur Sicherungskopie ändern möchten, klicken Sie auf die Schaltfläche **Kommentar ändern**. Wenn Sie die Sicherungskopie löschen möchten, klicken Sie auf **Löschen**.

Die Sicherungskopien der Konfiguration werden automatisch nach Erstellungsdatum oder nach Kommentaren sortiert. Zum Ändern der Sortierreihenfolge klicken Sie auf die Spaltenüberschrift **Erstellungszeit und -Datum** oder auf **Kommentar**.

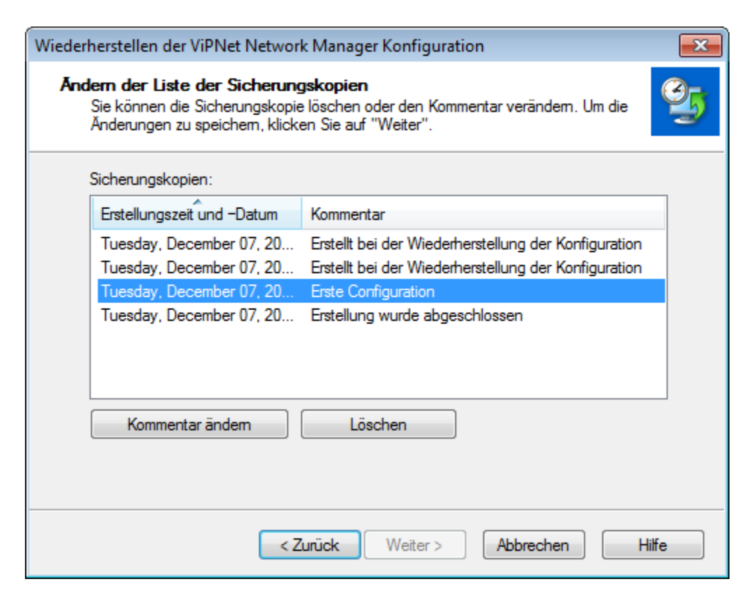


Abbildung 79. Liste der Sicherungskopien ändern

4 Klicken Sie auf **Weiter**, um die Bearbeitung abzuschließen.

5 Klicken Sie auf der Seite **Bearbeitung der Liste der Sicherungskopien abschließen** auf **Fertig**, um den Assistenten abzuschließen.

Wenn Sie die Arbeit mit Sicherungskopien fortsetzen möchten, klicken Sie auf **Zum Anfang**.

Letzte Wiederherstellung der Konfiguration rückgängig machen



Hinweis. Dieser Vorgang kann erst nach einer Wiederherstellung der Konfiguration aus einer Sicherungskopie erfolgen, wenn seitdem keine neuen Sicherungskopien der Konfiguration erstellt wurden.

Zum Widerrufen der letzten Wiederherstellung der Konfiguration:

1 Wählen Sie im Fenster des Programms ViPNet Network Manager im Menü **Extras** den Befehl **Sicherungskopien der Konfiguration**. Es wird der Assistent **Widerherstellung der ViPNet Network Manager Konfiguration**.

2 Wählen Sie auf der Seite **Wiederherstellung der ViPNet Network Manager Konfiguration** die Option **Die letzte Wiederherstellung widerrufen** und klicken anschließend auf **Weiter**.

Der Widerruf der letzten Wiederherstellung der Konfiguration wird gestartet.

3 Klicken Sie auf der Seite **Widerruf der letzten Konfigurationswiederherstellung abschließen** auf die Schaltfläche **Schließen**, um den Assistenten abzuschließen.

Export und Import von ViPNet Network Manager-Konfigurationen

Bei Bedarf können Sie die Konfiguration des Programms ViPNet Network Manager in eine Datei exportieren oder aus einer Datei importieren.

Die Import- und Exportfunktionalität der ViPNet Network Manager-Konfiguration kann insbesondere in folgenden Fällen von Nutzen sein:

- Übertragung des Programms ViPNet Network Manager mitsamt aller Einstellungen und ViPNet Netzwerkparameter auf einen neuen Computer. Dazu:
  - Führen Sie auf dem alten Computer den Export der ViPNet Network Manager-Konfiguration durch (s. Export der Konfiguration auf S. 161).
  - Installieren Sie ViPNet Network Manager auf dem neuen Computer (s. Installation von ViPNet Network Manager auf S. 53).
  - Importieren Sie auf dem neuen Computer die Konfiguration aus der vorher erstellten Exportdatei (s. Import der Konfiguration auf S. 161).
  - Registrieren Sie das Programm ViPNet Network Manager (s. Registrierung von ViPNet Network Manager auf S. 70).
- Erstellung einer Sicherungskopie der ViPNet Network Manager-Konfiguration für den Fall, dass es zu Ausfällen der Hard- oder Software kommt. Exportieren Sie dazu die Programmkonfiguration auf einen externen Datenträger und bewahren Sie diesen an einem sicheren Ort auf.



Hinweis. Wenn aktuelle Programm- und ViPNet Netzwerkparameter von ViPNet Network Manager gesichert werden sollen, um bei Bedarf Änderungen wieder rückgängig machen zu können, dann benutzen Sie den Assistenten zum Erstellen einer Sicherungskopie der Konfiguration (s. Erstellen und Wiederherstellen von Sicherungskopien der ViPNet Network Manager-Konfiguration auf S. 153).

Wenn ab dem Zeitpunkt des Konfigurationsexports bis zum Zeitpunkt des Imports wesentliche Änderungen an der Hardware des betroffenen Computers durchgeführt wurden, dann sollte das Programm ViPNet Network Manager erneut registriert werden. Wenn keine Hardwareänderungen durchgeführt wurden, ist eine wiederholte Registrierung nicht erforderlich.

Die Konfigurationsdatei von ViPNet Network Manager hat die Erweiterung `.rps` und enthält alle Daten, die für das Wiederherstellen der Funktionsfähigkeit des Programms ViPNet Network Manager und des ViPNet Netzwerks benötigt werden: eigene Netzwerkstruktur, Informationen über Partnernetzwerke, Lizenz- und Registrierungsdaten u. s. w.

Export der Konfiguration

Führen Sie folgende Schritte durch, um die ViPNet Network Manager-Konfiguration in eine Datei zu exportieren:

1 Wählen Sie im Programmfenster von ViPNet Network Manager im Menü **Extras** den Eintrag **Export der Konfiguration**.

2 Geben Sie im Fenster **Export der Konfiguration** den Dateinamen und den Ordner für die Speicherung der Sicherungskopie der Konfiguration an und klicken anschließend auf **Speichern**.

3 Nach erfolgreichem Speichern der Sicherungskopie wird eine entsprechende Meldung eingeblendet. Klicken Sie im Meldungsfenster auf **OK**.

   Im gewählten Ordner wird eine Datei mit der Erweiterung `.rps` erstellt, die eine Sicherungskopie der aktuellen ViPNet Network Manager-Konfiguration sowie früher angelegte Sicherungskopien der Konfiguration enthält.

Import der Konfiguration

Führen Sie folgende Schritte durch, um die ViPNet Network Manager-Konfiguration aus einer Datei zu importieren:

1 Wählen Sie im Programmfenster von ViPNet Network Manager im Menü **Extras** den Eintrag **Import der Konfiguration**.

2 Geben Sie im Fenster **Import der Konfiguration** eine Datei mit der Erweiterung `*.rps` an, die eine passende Sicherungskopie der ViPNet Network Manager-Konfiguration enthält, und klicken auf die Schaltfläche **Öffnen**.

   Es wird der Assistent **Wiederherstellen der ViPNet Network Manager Konfiguration** gestartet.

3 Wählen Sie auf der ersten Seite des Assistenten die Option **ViPNet Network Manager Konfiguration wiederherstellen** und klicken auf **Weiter**.

   Es wird die Seite **Auswahl der Sicherungskopie** (s. Abbildung 77 auf S. 156) geöffnet, auf der eine Liste aller Konfigurationen angezeigt wird, die in der gewählten Exportdatei enthalten sind.

4 Geben Sie die Sicherungskopie der Konfiguration an, die wiederhergestellt werden soll, und klicken auf **Weiter**.

5 Wenn sich das aktuelle Administratorpasswort von ViPNet Network Manager vom in der gewählten Konfiguration gespeicherten Passwort unterscheidet, dann geben Sie auf der Seite **Passwort** das Passwort ein, das zum Zeitpunkt der Speicherung der Sicherungskopie gültig war, und klicken auf **Weiter**.

6 Klicken Sie nach erfolgreichen Wiederherstellung der Konfiguration auf der letzten Seite des Assistenten auf **Schließen**. Das Programm ViPNet Network Manager wird neu gestartet.

Beim Importieren einer ViPNet Network Manager-Konfiguration werden alle Programmeinstellungen und ViPNet Netzwerkparameter wiederhergestellt, die in der gewählten Sicherungskopie gespeichert sind.

Daneben werden auch die ViPNet Netzwerknummer und die Lizenz- und Registrierungsdaten aus der Sicherungskopie wiederhergestellt. Wenn aber seit dem Zeitpunkt des Konfigurationsexports wesentliche Änderungen an der Hardware des Computers vorgenommen wurden oder wenn der Konfigurationsexport selbst auf einem anderen Computer durchgeführt wurde, dann sollte das Programm erneut registriert werden (s. Registrierung von ViPNet Network Manager auf S. 70).

Beim Import der Konfiguration aus der Datei wird eine Sicherungskopie der aktuellen Konfiguration des Programms angelegt. Nach dem Import stehen alle ViPNet Network Manager-Konfigurationen, die in der gewählten Datei `*.rps` gespeichert wurden, für eine mögliche Wiederherstellung mit Hilfe des Assistenten **Wiederherstellen der ViPNet Network Manager Konfiguration** zur Verfügung.

Neuerstellen des Netzwerkes

Gehen Sie wie folgt vor, um ein ViPNet Netzwerk neu zu erstellen:

1 Führen Sie einen der folgenden Schritte durch:

- Wählen Sie im Menü **Netzwerk** den Befehl **Erstellen**.
- Wählen Sie in der Navigationsleiste den Knoten **Eigenes Netzwerk**. Klicken Sie dann in der Panel-Ansicht auf die Schaltfläche **Netzwerk erstellen**.

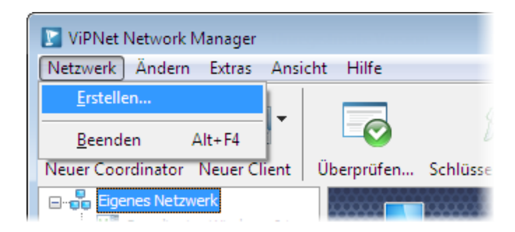


Abbildung 80. Neuerstellung des ViPNet-Netzwerks

2 Es wird eine Meldung angezeigt, dass die Struktur des vorher erstellten Netzwerks gelöscht wird.



Achtung! Die Struktur und die Einstellungen des aktuellen ViPNet Netzwerks werden gelöscht. Ebenso wird ein Wechsel des Administratorpassworts wie beim ersten Start des Programms ViPNet Network Manager erforderlich. Die Registrierungsdaten des Programms bleiben unverändert.

Vor dem Erstellen eines neuen Netzwerks wird eine Sicherungskopie der laufenden Netzwerkkonfiguration erzeugt (s. Erstellen und Wiederherstellen von Sicherungskopien der ViPNet Network Manager-Konfiguration auf S. 153). Im Falle der Wiederherstellung des alten ViPNet Netzwerks muss das Passwort des ViPNet Network Manager-Administrators eingegeben werden, welches zum Zeitpunkt der Erstellung der Sicherungskopie aktuell war.

Klicken Sie im Fenster mit der Meldung auf **Ja**.

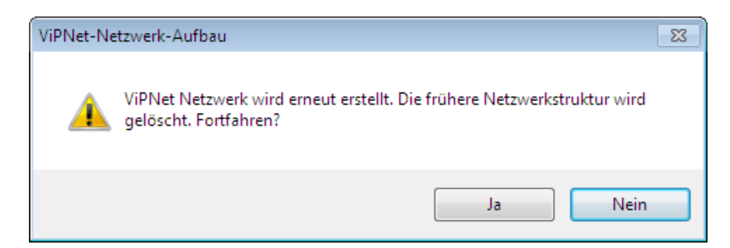


Abbildung 81. Existierende Netzwerkstruktur wird gelöscht

3 Das Programm ViPNet Network Manager wird neu gestartet, dabei wird das Fenster **ViPNet Network Manager Passwort** (s. Abbildung 28 auf S. 84) angezeigt.

Geben Sie das Passwort ein, das für die Anmeldung im Programm ViPNet Network Manager verwendet werden soll. In der Liste **Passworttyp** können die Optionen **Benutzerdefiniert** oder **Zufällig** ausgewählt werden. Nachdem Sie das Passwort erstellt haben, klicken Sie auf **OK**. Es wird der ViPNet Netzwerkaufbau Assistent gestartet.

4 Erstellen Sie eine neue Netzwerkstruktur mit Hilfe des ViPNet Netzwerkaufbau Assistenten (s. Automatische Generierung der ViPNet Netzwerkstruktur auf S. 86).



Partnernetzwerk-Verbindungen

Partnernetzwerk-Verbindungen. Kurzer Überblick



Hinweis. In der Demoversion von ViPNet VPN kann keine Partner-Netzwerkverbindung aufgebaut werden. Wenn Sie Verbindungen zu einem Partnernetzwerk aufbauen möchten, dann erwerben Sie eine Vollversion von ViPNet VPN, indem Sie Ihr Programm registrieren (s. Registrierung von ViPNet Network Manager auf S. 70).

Fast alle Computer sind in unterschiedlichen Netzwerken integriert. Durch Verbindungen zwischen diesen Netzwerken können die Benutzer miteinander kommunizieren, Daten austauschen und gemeinsame Projekte verwirklichen.

Virtuelle private Netzwerke (VPN – Virtual Private Network) ermöglichen den Aufbau von verschlüsselten Verbindungen zwischen Computern, die zu unterschiedlichen Netzwerken gehören. Dadurch kann die Vertraulichkeit der Daten während der Übertragung zuverlässig geschützt werden.

Mit Hilfe der ViPNet Technologie kann ein eigenes VPN aufgebaut und Verbindungen zu anderen ViPNet Netzwerken hergestellt werden, um eine sichere Arbeitsumgebung für den Austausch von Daten, Dateien, Nachrichten, u. s. w. zu schaffen. ViPNet Netzwerke, die Teil einer solchen Umgebung sein sollen, können sich in verschiedenen Städten oder sogar Ländern befinden und beliebig weit voneinander entfernt sein. Die einzige Voraussetzung für die Verbindung ist der Anschluss an das Internet.

Um Ihr ViPNet Netzwerk mit einem anderen ViPNet Netzwerk zu verbinden (im Weiteren werden solche Netzwerke als Partnernetzwerke bezeichnet), sollte zwischen den beiden Netzwerken eine Partnernetzwerk-Verbindung eingerichtet werden. Durch Partnernetzwerk-Verbindungen kann eine beliebige Anzahl an Netzwerken miteinander verbunden werden.



Achtung! Wenn in Ihrem Netzwerk ein Coordinator als Manager-Arbeitsplatz eingerichtet ist, dann können Partnernetzwerk-Verbindungen ausschließlich mit ViPNet VPN-Netzwerken der Version 3.0.4 oder höher hergestellt werden.

Es gibt zwei Methoden, Partnernetzwerk-Verbindungen einzurichten, je nachdem, wer die Partnernetzwerk-Verbindung initiiert. Im Übrigen sind sich beide Verbindungswege sehr ähnlich.

Aufbau von Partnernetzwerk-Verbindungen

Führen Sie die folgenden Schritte durch, um die Verbindung mit einem Partnernetzwerk aufzubauen:

- Wenn die Partnernetzwerk-Verbindung von Ihnen initiiert wird:
    - Erstellen Sie eine Datei mit Informationen zu Ihren Netzwerk und überreichen Sie diese auf einem externen Datenträger dem Administrator des ViPNet Netzwerks, zu dem die Verbindung aufgebaut werden soll.
    - Der Administrator des anderen ViPNet Netzwerks bearbeitet die erhaltene Datei mit den Partnernetzwerk-Informationen und erstellt eine neue Datei mit Angaben zu seinem Netzwerk. Diese Datei überreicht er Ihnen.
    - Bearbeiten Sie die erhaltene Datei mit den Partnernetzwerk-Informationen, erstellen und versenden Sie aktualisierte Schlüsseldistributionen an alle Netzwerkknoten Ihres Netzwerks, die mit dem Partnernetzwerk kommunizieren sollen.
- Wenn die Verbindung vom Administrator eines anderen ViPNet Netzwerks initiiert wird:
    - Sie erhalten eine Datei mit den Partnernetzwerk-Informationen vom Administrator des anderen ViPNet Netzwerks.
    - Bearbeiten Sie die erhaltene Datei mit den Partnernetzwerk-Informationen. Erstellen Sie eine Datei mit den Angaben zu Ihrem Netzwerk.
    - Überreichen Sie die erstellte Datei dem Administrator des anderen Netzwerks, der die Partnernetzwerk-Verbindung initiiert hat.
    - Erstellen Sie neue Schlüsseldistributionen für alle Netzwerkknoten Ihres Netzwerks, die mit dem Partnernetzwerk verbunden werden sollen, und versenden Sie diese.

Nach der Übernahme aller Änderungen können die Netzwerkknoten Ihres ViPNet Netzwerks Verbindungen zu den Netzwerkknoten des Partnernetzwerks aufbauen und mit ihnen Daten über einen gesicherten Kanal austauschen.

Auf der Abbildung unten wird die Reihenfolge der Schritte beim Aufbau der Partnernetzwerk-Kommunikation anschaulich dargestellt. Anschließend wird dieser Vorgang im Detail beschrieben.

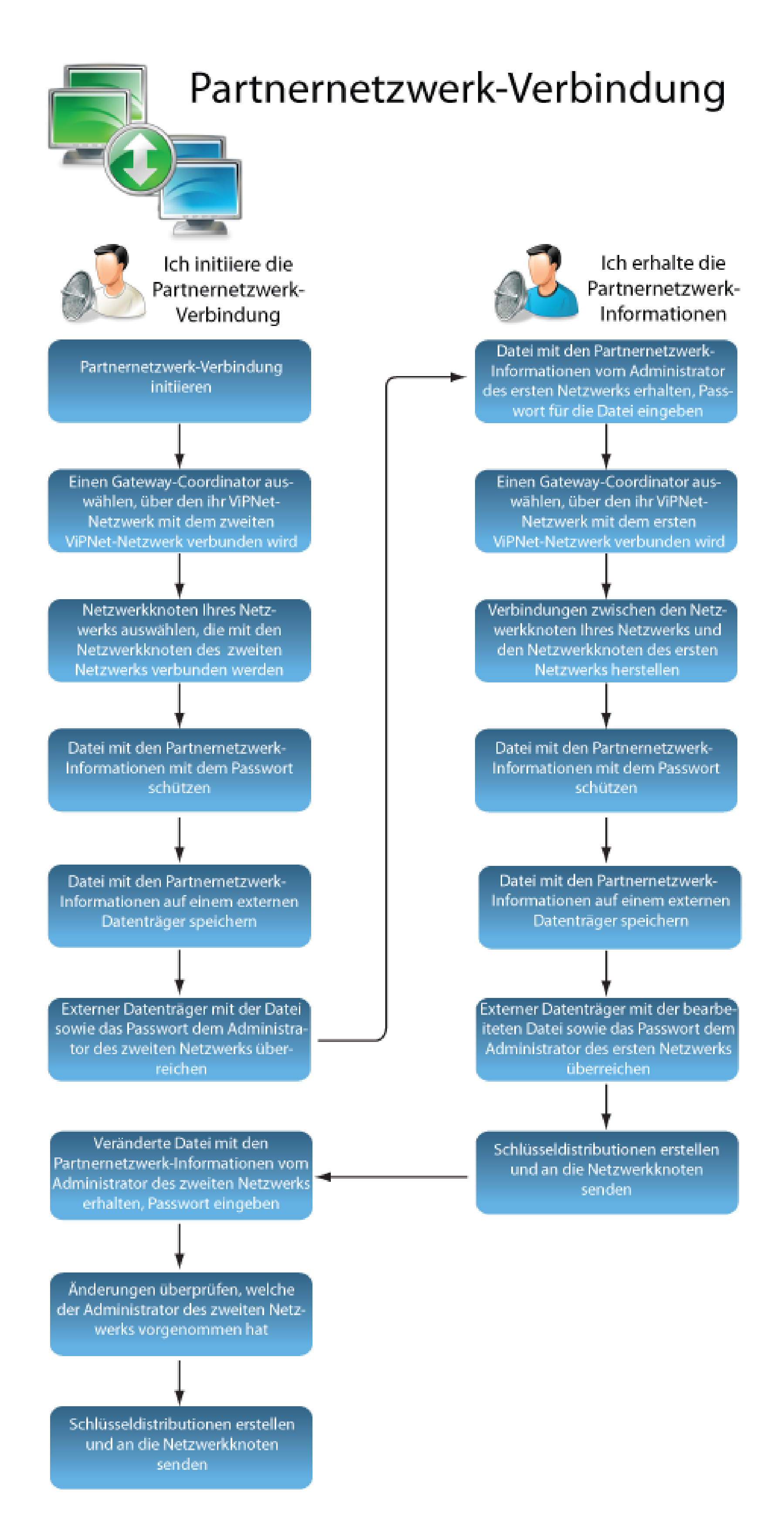


Abbildung 82. Partnernetzwerk-Verbindung aufbauen

Initiierung der Partnernetzwerk-Verbindung

Wenn Sie eine Verbindung zu einem anderen ViPNet Netzwerk initiieren möchten, dann sollten Sie:

- eine Datei mit den Partnernetzwerk-Informationen zu Ihrem Netzwerk erstellen;
- ein Passwort zum Schutz der Partnernetzwerk-Informationen erstellen;
- die Partnernetzwerk-Datei auf einem externen Datenträger speichern;
- den externen Datenträger und das Passwort an den Administrator des anderen ViPNet Netzwerks überreichen.

Zum Initiieren der Partnernetzwerk-Verbindung:

1 Klicken Sie in der Symbolleiste auf die Schaltfläche **Netz. Verb**. Der Assistent zum Aufbau einer Partnernetzwerk-Verbindung wird geöffnet.

2 Wählen Sie im Fenster **Partnernetzwerk-Verbindung** die Option **Ich initiiere die Partnernetzwerk-Verbindung** und klicken auf **Weiter**.

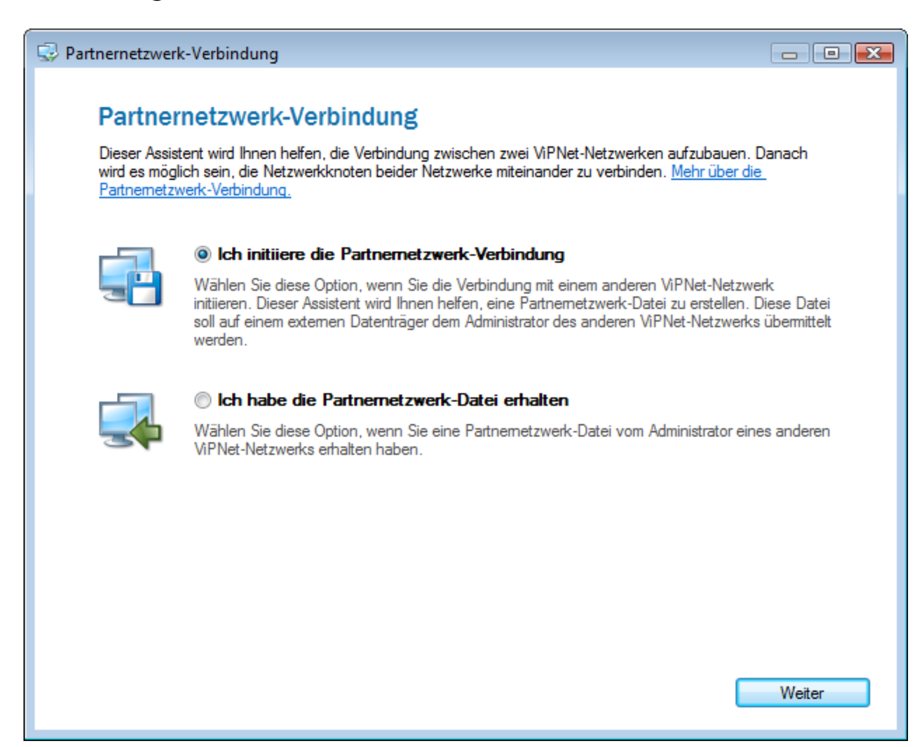


Abbildung 83. Assistent zum Aufbau von Partnernetzwerk-Verbindungen

3 Machen Sie im nächsten Fenster des Assistenten Angaben zum ViPNet Netzwerk, zu dem die Verbindung aufgebaut werden soll. Diese Angaben sollten die folgenden Daten beinhalten:

  - Nummer des ViPNet Netzwerks;
  - Name des ViPNet Netzwerks. Dieser Name wird in der Netzwerkstruktur in der Navigationsleiste angezeigt. Sie können einen beliebigen Namen wählen. Anderenfalls wird der Name automatisch vom System im Format „Netzwerk <Netzwerknummer>“ definiert.

Nachdem Sie alle notwendigen Information eingegeben haben, klicken Sie auf **Weiter**.

4 Wählen Sie im Fenster **Gateway-Coordinator des eigenen ViPNet Netzwerks** in der Liste einen Gateway-Coordinator des eigenen Netzwerks aus, über den Ihr ViPNet Netzwerk mit dem anderen ViPNet Netzwerk verbunden werden soll. Klicken Sie dann auf **Weiter**.

5 Verwenden Sie im Fenster **Netzwerkknoten, welche für den Verbindungsaufbau zur Verfügung stehen** die Schaltflächen **Hinzufügen** oder **Entfernen** dazu, die Netzwerkknoten Ihres Netzwerks festzulegen, die mit den Netzwerkknoten des anderen Netzwerks verbunden werden sollen. Klicken Sie anschließend auf **Weiter**.

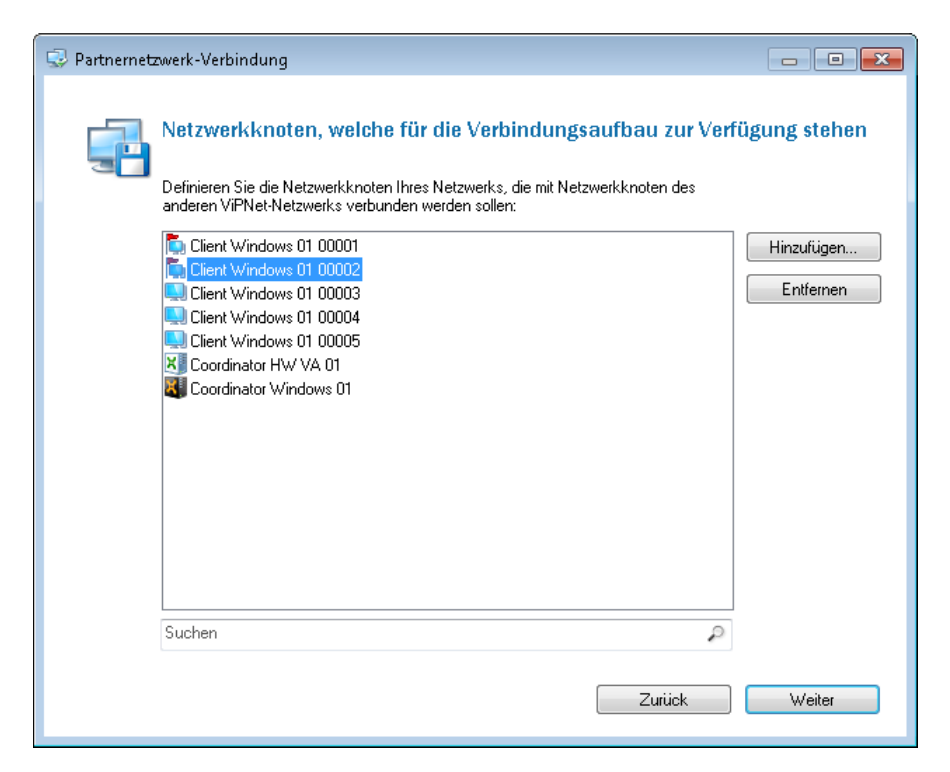


Abbildung 84. Netzwerkknoten, welche für den Verbindungsaufbau zur Verfügung stehen

6 Geben Sie im Fenster **Passwort für Partnernetzwerk-Informationen** ein Passwort ein und bestätigen es.



Achtung! Das Passwort sollte zwischen 6 und 32 Zeichen lang sein. Das Passwort sollte zusammen mit der Datei mit den Partnernetzwerk-Informationen an den Administrator des anderen ViPNet Netzwerks übergeben werden.

7 Klicken Sie im Fenster **Partnernetzwerk-Informationen auf externem Datenträger speichern** auf **Durchsuchen** und geben den Dateinamen und den Pfad für die Datei mit den Partnernetzwerk-Informationen an.

Im Feld **Nachricht für den Netzwerkadministrator des anderen Netzwerks** können Sie bei Bedarf einen Kommentar für den Administrator des anderen Netzwerks eingeben.



Hinweis. Der Dateiname für die Datei der Partnernetzwerk-Informationen wird vom System automatisch vorgeschlagen. Bei Bedarf können Sie diesen Dateinamen ändern.

8 Klicken Sie auf **Weiter**. Die Datei mit den Partnernetzwerk-Informationen wird im angegebenen Ordner erstellt.

   Falls das digitale Roulette in der aktuellen Sitzung von ViPNet Network Managers noch nicht verwendet wurde, wird es beim Speichern der Datei mit den Partnernetzwerk-Informationen angezeigt. Folgen Sie in diesem Fall den Anweisungen im Fenster **Digitales Roulette**.

9 Klicken Sie im Fenster **Partnernetzwerk-Informationen werden auf externem Datenträger gespeichert** auf **Fertig**.

10 Übergeben Sie die Datei mit den Partnernetzwerk-Informationen und das dazugehörige Passwort dem Administrator des ViPNet Netzwerks, zu dem Partnernetzwerk-Verbindungen hergestellt werden sollen.



Hinweis. Der Administrator des ViPNet Netzwerks, mit dem eine Partnernetzwerk-Verbindung eingerichtet werden soll, sollte die von Ihnen überreichte Datei mit den Partnernetzwerk-Informationen annehmen und verarbeiten. Anschließend sollte er eine Datei erstellen, welche Informationen zu seinem Netzwerk enthält, und diese Datei an Sie überreichen.

Nachdem die Datei mit den Partnernetzwerk-Informationen erstellt wurde, erscheint im Programmfenster von ViPNet Network Manager in der Navigationsleiste der Ordner **Partnernetzwerke**. Dort befindet sich ein weiterer Ordner mit dem Namen des Netzwerks, der im Assistenten **Partnernetzwerk-Verbindung** definiert wurde.

Annahme und Verarbeitung von Partnernetzwerk-Informationen

Wenn die Partnernetzwerk-Verbindung vom Administrator des anderen ViPNet Netzwerks initiiert wurde, überreicht er Ihnen die Datei mit den Partnernetzwerk-Informationen und das dazugehörige Passwort.

Starten Sie nach dem Erhalt der Datei mit den Partnernetzwerk-Informationen und des Passworts den Assistenten **Partnernetzwerk-Verbindung** und führen die folgenden Schritte durch.

Zum Annehmen der Datei mit den Partnernetzwerk-Informationen:

1 Klicken Sie in der Symbolleiste von ViPNet Network Manager auf die Schaltfläche **Netz. Verb**. Der Assistent zum Aufbau einer Partnernetzwerk-Verbindung wird geöffnet.

2 Wählen Sie auf der Seite **Partnernetzwerk-Verbindung** (s. Abbildung 83 auf S. 169) die Option **Ich habe die Datei mit den Partnernetzwerk-Informationen erhalten** und klicken auf **Weiter**.

3 Klicken Sie auf der Seite **Datei mit den Partnernetzwerk-Informationen angeben** auf die Schaltfläche **Durchsuchen** und geben den Pfad zur Datei mit den Partnernetzwerk-Informationen an.

Sobald eine Datei mit den Partnernetzwerk-Informationen ausgewählt ist, werden im Assistentenfenster der Pfad zur gewählten Datei, die Nummer des anderen Netzwerks und der Kommentar des Administrators angezeigt.

Klicken Sie auf **Weiter**.

4 Geben Sie auf der Seite **Passwort eingeben** das Passwort für die Datei mit den Partnernetzwerk-Informationen ein und klicken auf **Weiter**. Das Passwort erhalten Sie vom Administrator des Netzwerks, der die Datei mit den Partnernetzwerk-Informationen erstellt hat.

5 Geben Sie auf der Seite **Angaben zum anderen ViPNet Netzwerk** den Namen an, unter dem das Partnernetzwerk in der Navigationsleiste angezeigt werden soll, und klicken auf **Weiter**.

6 Wählen Sie auf der Seite **Gateway-Coordinator des eigenen ViPNet Netzwerks** einen Gateway-Coordinator, über den Ihr ViPNet Netzwerk mit dem anderen ViPNet Netzwerk verbunden werden soll, und klicken auf **Weiter**.

7 Verwenden Sie auf der Seite **Netzwerkknoten, welche für den Verbindungsaufbau zur Verfügung stehen** (s. Abbildung 84 auf S. 170) die Schaltfläche **Hinzufügen** oder **Entfernen** dazu, die Netzwerkknoten Ihres Netzwerks festzulegen, die mit den Netzwerkknoten des anderen Netzwerks verbunden werden sollen. Klicken Sie anschließend auf **Weiter**.

8 Definieren Sie auf der Seite **Verbindungen mit anderen ViPNet Netzwerken** die Verbindungen zwischen den Netzwerkknoten Ihres Netzwerks und den Knoten des Partnernetzwerks. Wählen Sie dafür einen Netzwerkknoten in der linken Fensterhälfte und editieren die Verbindungen mit Hilfe der Schaltflächen **Hinzufügen** und **Entfernen**.

Nachdem alle Verbindungen definiert wurden, klicken Sie auf **Weiter**.

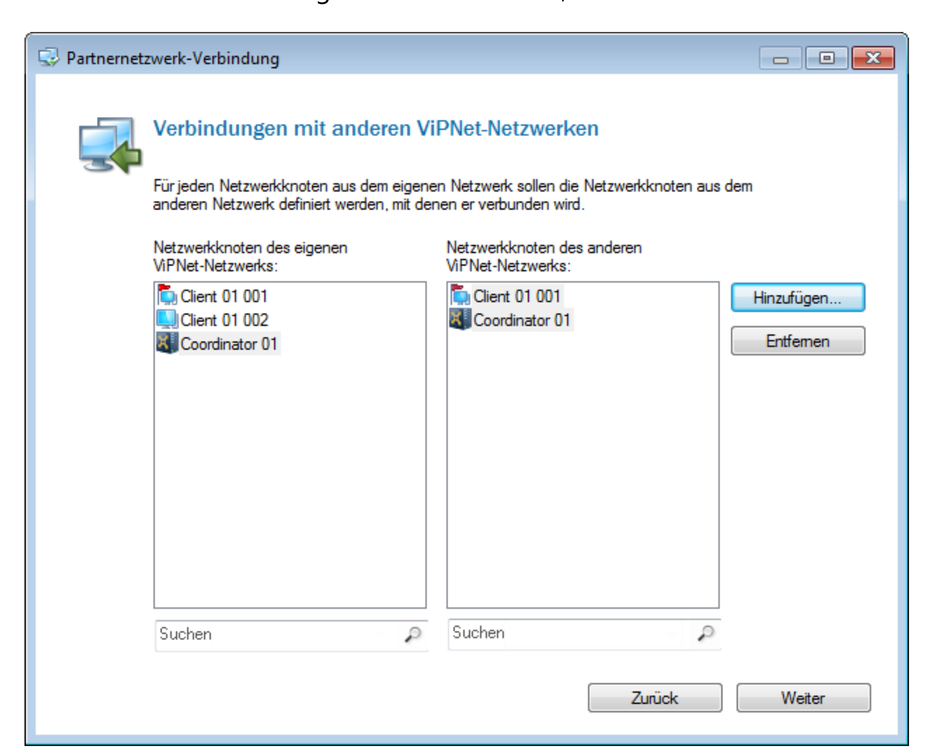


Abbildung 85. Verbindungen mit anderen ViPNet Netzwerkknoten editieren

9 Auf der Seite **Partnernetzwerk-Informationen auf externem Datenträger speichern** klicken Sie auf **Durchsuchen** und geben den Dateinamen und den Pfad für die Datei mit den Partnernetzwerk-Informationen ein.

Im Feld **Nachricht für den Netzwerkadministrator des anderen Netzwerks** schreiben Sie bei Bedarf eine Nachricht an den Administrator des anderen Netzwerks.

10 Klicken Sie auf **Weiter**. Die Datei mit den Partnernetzwerk-Informationen wird gespeichert.

11 Auf der Seite **Partnernetzwerk-Informationen werden auf externem Datenträger gespeichert** markieren Sie das Kontrollkästchen **Schlüsseldistribution erstellen und senden (empfohlen)** und klicken auf **Fertig**.

Nach dem Beenden der Arbeit im Assistenten werden die Schlüsseldistributionen für die Netzwerkknoten Ihres Netzwerks erstellt und versendet.

12 Senden Sie dem Administrator des anderen Netzwerks auf sicherem Wege (z.B. per Post) die Datei mit den Partnernetzwerk-Informationen mit dem neuen Passwort zurück.

Nachdem die Datei mit den Partnernetzwerk-Informationen bearbeitet wurde, erscheint im Programmfenster von ViPNet Network Manager in der Navigationsleiste der Knoten **Partnernetzwerke**. Dort befindet sich ein weiterer Knoten mit dem Namen des Netzwerks, der im Assistenten **Partnernetzwerk-Verbindung** definiert wurde.



Hinweis. Damit der Aufbau der Partnernetzwerk-Verbindung fertiggestellt wird, sollte die erstellte Datei mit den Partnernetzwerk-Informationen und das dazugehörige Passwort an den Administrator des ViPNet Netzwerks weitergeleitet werden, der die Partnernetzwerk-Verbindung initiiert hat. Erst dann wird die Verbindung endgültig eingerichtet und die Netzwerkknoten des Partnernetzwerks werden erreichbar.

Fertigstellung der Partnernetzwerk-Verbindung

Nach der Initiierung der Partnernetzwerk-Verbindung haben Sie die Datei mit den Partnernetzwerk-Informationen und das Passwort dazu erstellt und dem Administrator des anderen ViPNet Netzwerks überreicht. Der Administrator des anderen Netzwerks hat die Datei bearbeitet und Ihnen seinerseits eine Datei mit Informationen zu seinem Netzwerk überreicht. Nun ist es notwendig, die erhaltene Datei anzunehmen und zu bearbeiten.

Führen Sie zum Fertigstellen der Partnernetzwerk-Verbindung die folgenden Schritte durch:

1 Klicken Sie in der Symbolleiste von ViPNet Network Manager auf die Schaltfläche **Netz. Verb.** Der Assistent zum Aufbau einer Partnernetzwerk-Verbindung wird geöffnet.

2 Wählen Sie auf der Seite **Partnernetzwerk-Verbindung** (s. Abbildung 83 auf S. 169) die Option **Ich habe die Datei mit der Partnernetzwerk-Informationen erhalten** aus und klicken auf **Weiter**.

3 Klicken Sie auf der Seite **Partnernetzwerk-Informationen angeben** auf die Schaltfläche **Durchsuchen** und geben den Speicherort der Datei mit den Partnernetzwerk-Informationen an.

Sobald eine Datei mit Partnernetzwerk-Informationen ausgewählt ist, werden auf der Seite des Assistenten der Pfad, die Nummer des anderen Netzwerks und der Kommentar des Administrators angezeigt.

Klicken Sie auf **Weiter**.

4 Machen Sie sich auf der Seite **Partnernetzwerk-Informationen wurden vom Administrator des anderen ViPNet Netzwerks geändert** mit den Änderungen der Partnernetzwerk-Informationen vertraut, die der Administrator des anderen Netzwerks vorgenommen hat, und klicken dann auf **Weiter**.

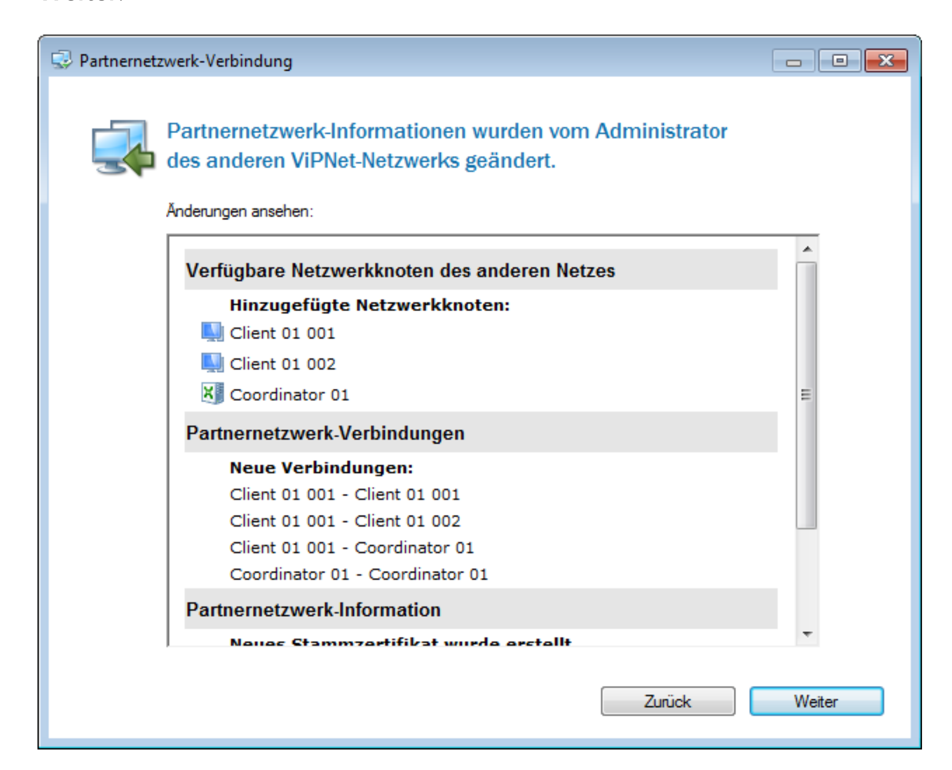


Abbildung 86. Änderungen in der Partnernetzwerk-Information

5 Auf der Seite **Verbindungen mit anderen ViPNet Netzwerken** (s. Abbildung 85 auf S. 172) können die Verbindungen zwischen den Netzwerkknoten des eigenen und des Partnernetzwerks gelöscht werden. Es können keine neuen Verbindungen hinzugefügt werden (die Schaltfläche **Hinzufügen** ist inaktiv). Nach dem Löschen einer Verbindung des eigenen Netzwerkknotens wird die Schaltfläche **Hinzufügen** für diesen Knoten wieder aktiv, die gelöschte Verbindung kann wiederhergestellt werden.

Nachdem Sie die Verbindungen bearbeitet haben, klicken Sie auf **Weiter**.

6 Aktivieren Sie auf der Seite **Partnernetzwerk-Informationen werden auf externem Datenträger gespeichert** das Kontrollkästchen **Schlüsseldistribution erstellen und senden (empfohlen)** und klicken dann auf **Fertig**.

Nach dem Beenden des Assistenten werden Schlüsseldistributionen für die Netzwerkknotens Ihres Netzwerks erstellt und versendet.



Hinweis. Damit die Schlüssel automatisch versendet werden, muss die ViPNet Software auf dem Manager-Arbeitsplatz richtig installiert und konfiguriert sein (s. Einrichtung des Manager-Arbeitsplatzes auf S. 53).

Stellen Sie sicher, dass auf dem Manager-Arbeitsplatz das Programm ViPNet Monitor gestartet ist. Dieses Programm startet regelmäßig das MFTP-Modul, das den Schlüsselversand durchführt.

Wenn alle Schritte richtig durchgeführt wurden, besteht nun eine voll funktionsfähige Partnernetzwerk-Verbindung zum gewählten ViPNet Partnernetzwerk.

Ändern von Partnernetzwerk-Verbindungen

Oft sollen Änderungen an den bestehenden Partnernetzwerk-Verbindungen vorgenommen werden. Es können die folgenden Änderungen erforderlich sein:

- zusätzlichen Netzwerkknoten des eigenen Netzwerks sollen Verbindungen zu den Netzwerkknoten des Partnernetzwerks ermöglicht werden;
- bestehende Verbindungen zwischen den Netzwerkknoten des eigenen Netzwerks und des Partnernetzwerks sollen geändert werden;
- der Gateway-Coordinator des eigenen Netzwerks soll geändert werden.

Beim Ändern der Partnernetzwerk-Verbindungen wird automatisch eine ausgehende Datei mit Partnernetzwerk-Informationen für alle Partnernetzwerke erstellt, die von den Änderungen betroffen sind. Damit die Änderungen übernommen werden, sollte die Datei mit den Partnernetzwerk-Informationen an die Administratoren der anderen ViPNet Netzwerke verschickt werden.



Hinweis. Die ausgehende Datei mit den Partnernetzwerk-Informationen wird automatisch bei Änderungen im eigenen Netzwerk erstellt, z.B. nach dem Löschen der Netzwerkknoten, welche eine Partnernetzwerk-Verbindung haben oder nach dem Ändern der Netzwerkknotenparameter (s. Konfiguration der Coordinatoren auf S. 109).

Durchführen von Änderungen im eigenen Netzwerk

Zum Ändern von Partnernetzwerk-Verbindungen:

1 Wählen Sie in der Navigationsleiste das Partnernetzwerk aus, dessen Verbindungsparameter geändert werden sollen.

2 Ändern Sie bei Bedarf die folgenden Parameter:

   - Netzwerkknoten des eigenen Netzwerks, die mit Netzwerkknoten des Partnernetzwerks verbunden sein können;
   - Verbindungen zwischen den Netzwerkknoten des eigenen Netzwerks und den Knoten des Partnernetzwerks;
   - Gateway-Coordinator,
   - Internetzwerk-Masterschlüssel.

Die Verbindungen zwischen den Netzwerkknoten des eigenen und des Partnernetzwerks ändern

Führen Sie die folgenden Schritte durch, um die Verbindungen zwischen den Netzwerkknoten des eigenen und des Partnernetzwerks zu ändern:

1 Wählen Sie in der Navigationsleiste einen Netzwerkknoten aus dem Partnernetzwerk aus, um seine Verbindungen zu bearbeiten.

2 Ändern Sie in der Panel-Ansicht mit Hilfe der Schaltflächen **Hinzufügen** oder **Entfernen** die Liste der Netzwerkknoten, die mit dem ausgewählten Partnernetzwerkknoten verbunden sind.

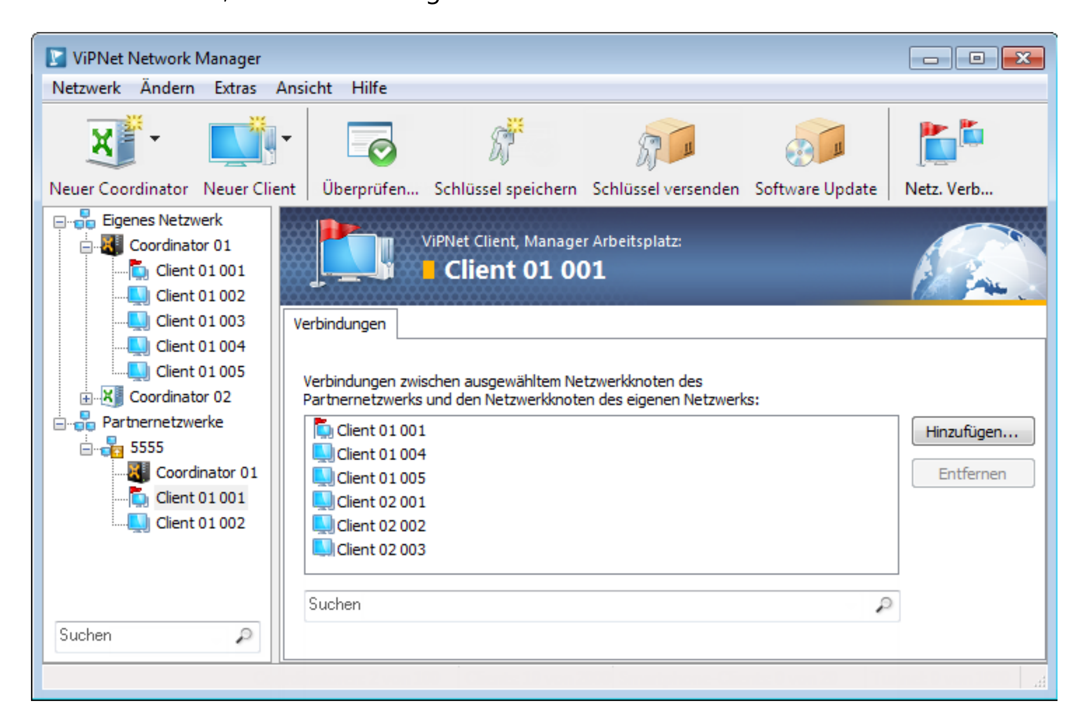


Abbildung 87. Verbindungen eines Netzwerkknotens im Partnernetzwerk

3 Wiederholen Sie bei Bedarf die Schritte 1 und 2 für die anderen Netzwerkknoten des Partnernetzwerks.

Die Netzwerkknoten des eigenen Netzwerks ändern, die mit dem Partnernetzwerk verbunden werden können

Zum Ändern der Liste der Netzwerkknoten im eigenen Netzwerk, die mit dem Partnernetzwerk verbunden werden können:

1 Wählen Sie in der Navigationsleiste das Partnernetzwerk aus, das bearbeitet werden soll.

2 Öffnen Sie in der Panel-Ansicht die Registerkarte **Netzwerkknoten des eigenen Netzwerks**.

3 Ändern Sie mit Hilfe der Schaltflächen **Hinzufügen** oder **Entfernen** die Liste der Netzwerkknoten des eigenen Netzwerks, die mit den Netzwerkknoten aus dem Partnernetzwerk verbunden werden können.

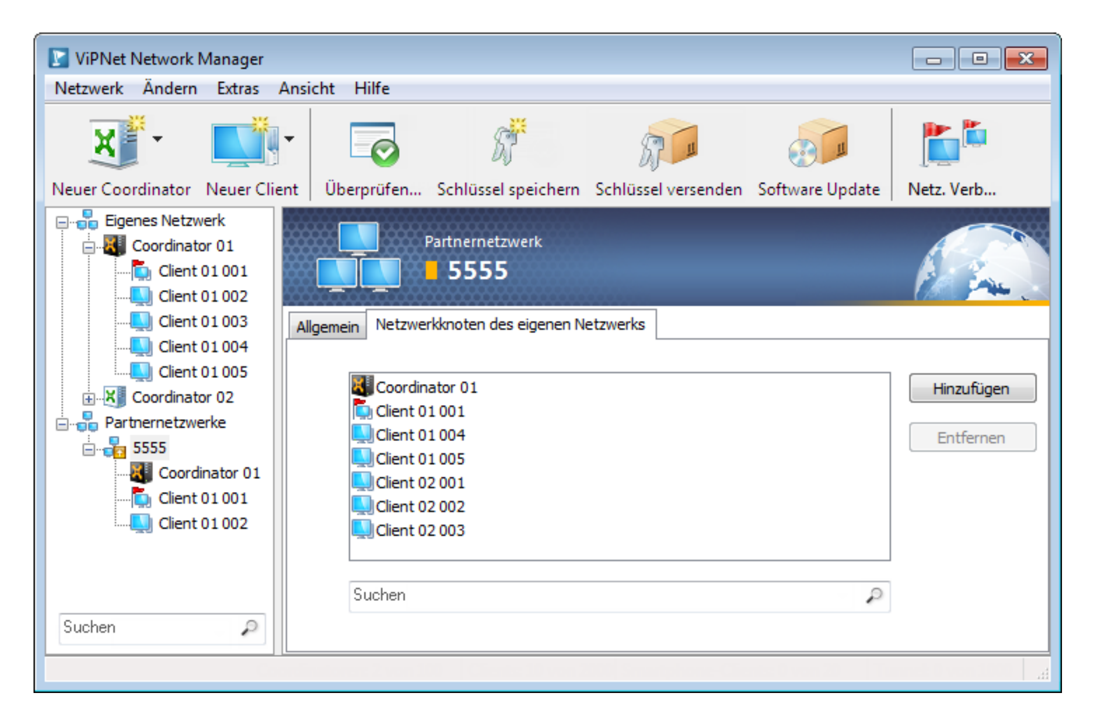


Abbildung 88. Liste der Netzwerkknoten des eigenen Netzwerks, die mit den Netzwerkknoten eines Partnernetzwerks verbunden werden können

Es sollte beachtet werden, dass beim Hinzufügen eines Netzwerkknotens zur Liste keine Verbindungen zwischen diesem Netzwerkknoten und den Netzwerkknoten anderer Netzwerke erstellt werden. Informationen zum Erstellen solcher Verbindungen finden Sie im Abschnitt Die Verbindungen zwischen den Netzwerkknoten des eigenen und des Partnernetzwerks ändern (auf S. 177).

Einen anderen Gateway-Coordinator für die Verbindung mit dem Partnernetzwerk definieren

Führen Sie die folgenden Schritte durch, um einen anderen Gateway-Coordinator für die Verbindungen mit dem Partnernetzwerk zu definieren:

1 Wählen Sie in der Navigationsleiste das Partnernetzwerk aus, für das ein anderer Gateway-Coordinator festgelegt werden soll.

2 Öffnen Sie in der Panel-Ansicht die Registerkarte **Allgemein**.

3 Wählen Sie in der Liste **Gateway-Coordinator des eigenen Netzwerks** den Coordinator aus, der für den Verbindungsaufbau mit dem Partnernetzwerk eingesetzt werden soll.

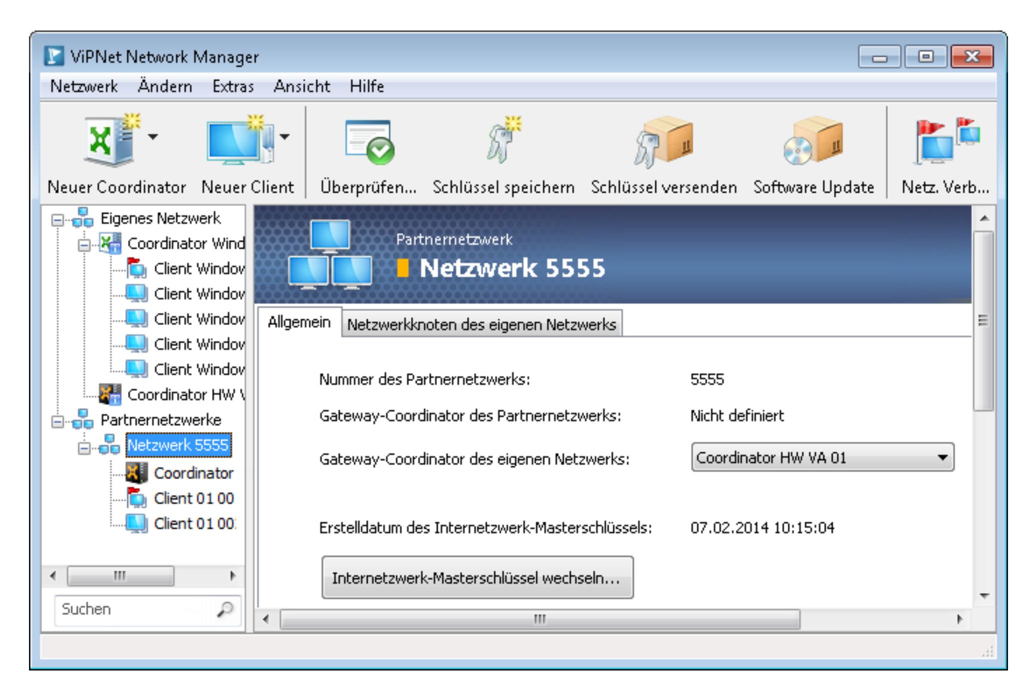


Abbildung 89. Gateway-Coordinator im eigenen Netzwerk definieren

Wechsel des Internetzwerk-Masterschlüssels

Damit die Zuverlässigkeit der Daten, die im Zuge von Partnernetzwerk-Verbindungen übermittelt werden, kontinuierlich gewährleistet werden kann, sollte der Internetzwerk-Masterschlüssel regelmäßig geändert werden.

Zum Ändern des Internetzwerk-Masterschlüssels (s. Internetzwerk-Masterschlüssel auf S. 371):

1 Wählen Sie in der Navigationsleiste das Partnernetzwerk aus, dessen Internetzwerk-Masterschlüssel gewechselt werden soll.

2 Öffnen Sie in der Panel-Ansicht die Registerkarte **Allgemein** (s. Abbildung 89 auf S. 179).

3 Klicken Sie auf die Schaltfläche **Internetzwerk-Masterschlüssel wechseln**.

4 Klicken Sie im Fenster zur Bestätigung auf **Ja**.

5 Klicken Sie im Fenster **Wechsel des Internetzwerk-Masterschlüssels** auf die Schaltfläche **Datei mit Partnernetzwerk-Informationen speichern**.

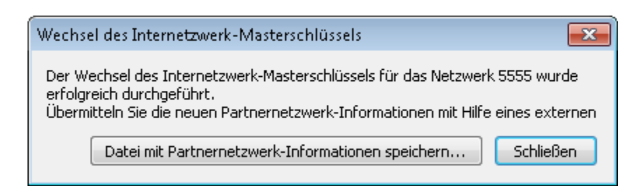


Abbildung 90. Fenster mit der Meldung über den erfolgreichen Wechsel des Masterschlüssels

6 Geben Sie im Fenster **Passwort für Partnernetzwerk-Informationen** ein Passwort ein und bestätigen es.



Achtung! Das Passwort sollte zwischen 6 und 32 Zeichen lang sein. Das Passwort sollte zusammen mit der Datei mit den Partnernetzwerk-Informationen an den Administrator des anderen ViPNet Netzwerks übergeben werden.

7 Klicken Sie im Fenster **Partnernetzwerk-Informationen auf externem Datenträger speichern** auf **Durchsuchen** und geben den Dateinamen und den Pfad für die Datei mit den Partnernetzwerk-Informationen an.

Im Feld **Nachricht für den Netzwerkadministrator des anderen Netzwerks** können Sie bei Bedarf einen Kommentar für den Administrator des anderen Netzwerks eingeben.



Hinweis. Der Dateiname für die Datei der Partnernetzwerk-Informationen wird vom System automatisch vorgeschlagen. Bei Bedarf können Sie diesen Dateinamen ändern.

8 Klicken Sie auf **Weiter**. Die Datei mit den Partnernetzwerk-Informationen wird im angegebenen Ordner erstellt.

Falls das digitale Roulette in der aktuellen Sitzung von ViPNet Network Managers noch nicht verwendet wurde, wird es beim Speichern der Datei mit den Partnernetzwerk-Informationen angezeigt. Folgen Sie in diesem Fall den Anweisungen im Fenster **Digitales Roulette**.

9 Klicken Sie im Fenster **Partnernetzwerk-Informationen werden auf externem Datenträger gespeichert** auf **Fertig**.

10 Übergeben Sie die Datei mit den Partnernetzwerk-Informationen und das dazugehörige Passwort dem Administrator des ViPNet Netzwerks, zu dem Partnernetzwerk-Verbindungen hergestellt werden sollen.

11 Der Administrator des Partnernetzwerks sollte das Update der Partnernetzwerk-Informationen übernehmen (s. Empfang von Änderungen der Partnernetzwerk-Informationen aus einem anderen ViPNet Netzwerk auf S. 182).

12 Versenden Sie Schlüsselupdates an die Knoten Ihres Netzwerks (s. Versenden der Schlüssel-Updates auf S. 145).

Innerhalb des Partnernetzwerks sollten ebenfalls Schlüsselupdates vom Netzwerkadministrator an die Knoten des Partnernetzwerks versendet werden.

Nach der Durchführung der aufgelisteten Schritte erfolgt die Kommunikation zwischen Ihrem Netzwerk und dem Partnernetzwerk unter Verwendung des neuen Masterschlüssels.

Versenden von Änderungen der Partnernetzwerk-Informationen

Nach Durchführung von Änderungen im eigenen Netzwerk werden automatisch Partnernetzwerk-Informationen für alle Partnernetzwerke erstellt, die von den Änderungen betroffen sind. In der Navigationsleiste wird neben den Namen dieser Partnernetzwerke das Symbol für ausgehende

Partnernetzwerk-Informationen angezeigt. Dieses Symbol wird auch in der Registerkarte **Ausgehende Partnernetzwerk-Information** angezeigt.

Führen Sie die folgenden Schritte durch, um ausgehende Partnernetzwerk-Informationen an die Partnernetzwerke zu senden:

1 Wählen Sie in der Navigationsleiste den Knoten **Partnernetzwerke**.

2 Öffnen Sie in der Panel-Ansicht die Registerkarte **Ausgehende Partnernetzwerk-Information**.

3 Wählen Sie in der Liste das Partnernetzwerk aus, an das Sie die Änderungen versenden möchten. Der Eintrag sollte durch das Symbol gekennzeichnet sein, der Status der ausgehenden Partnernetzwerk-Information sollte **Nicht gesendet** lauten. Klicken Sie auf die Schaltfläche **Senden**.

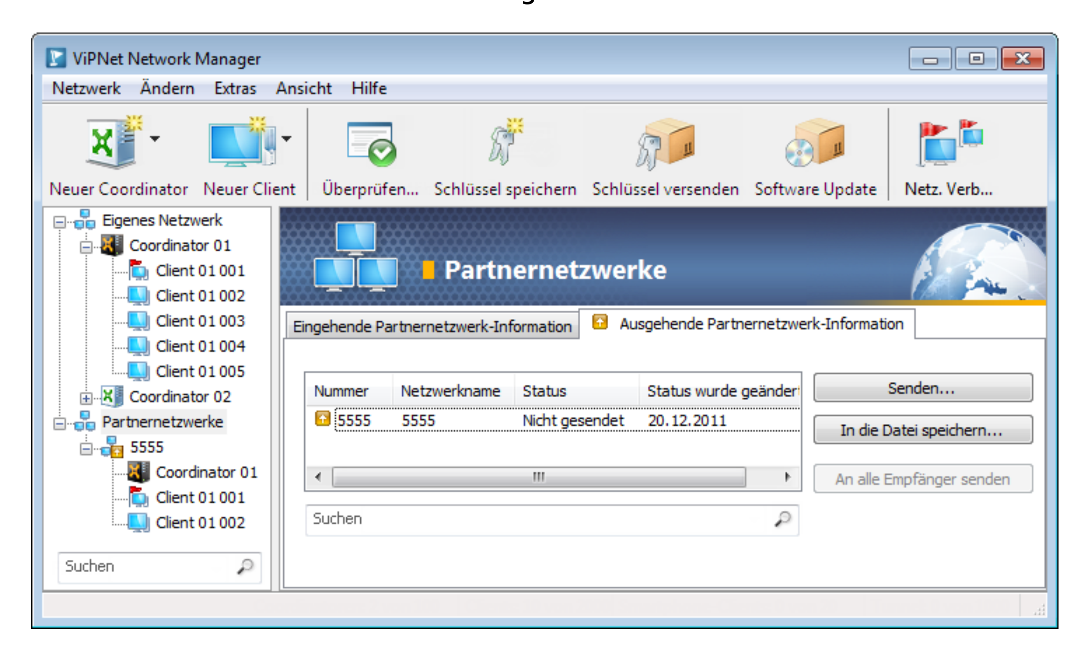


Abbildung 91. Ausgehende Partnernetzwerk-Information

4 Geben Sie im Fenster **Partnernetzwerk-Informationen versenden** einen Kommentar für den Systemadministrator des anderen ViPNet Netzwerks ein und klicken auf **Weiter**.



Hinweis. Wenn die Partnernetzwerk-Informationen für mehrere Netzwerke erstellt wurden und kein Bedarf besteht, etwaige Kommentare für die Netzwerkadministratoren dieser Netzwerke zu schreiben, können die Partnernetzwerk-Informationen gleichzeitig an alle Administratoren verschickt werden. Klicken Sie dazu auf die Schaltfläche **An alle Empfänger senden**.

Wenn keine sichere Verbindung über das MFTP–Modul sichergestellt werden kann, können Sie die Partnernetzwerk-Informationen in einer Datei speichern und diese dem Administrator des anderen Netzwerks auf einem externen Datenträger übergeben. Klicken Sie dazu auf die Schaltfläche **In die Datei speichern**.

5 Aktivieren Sie im Fenster **Partnernetzwerk-Informationen werden versendet** das Kontrollkästchen **Schlüsseldistribution erstellen und senden (empfohlen)**. Die Schlüsseldistributionen können auch später erstellt und versendet werden, aber dann treten die Änderungen in Ihrem Netzwerk erst nach dem Versand der Schlüssel in Kraft. Weitere Details über das Versenden der Schlüsseldistributionen finden Sie im Abschnitt Versenden der Schlüssel-Updates (auf S. 145).

Klicken Sie auf **Fertig**.



Achtung! Stellen Sie sicher, dass auf dem Manager-Arbeitsplatz das Programm ViPNet Monitor gestartet ist. Dieses Programm startet regelmäßig das ViPNet MFTP-Modul, das den Versand der Schlüsseldistributionen durchführt.

6 Die Änderungen in den Partnernetzwerk-Informationen werden an das andere Netzwerk versendet. Das Symbol der ausgehenden Partnernetzwerk-Informationen neben dem Namen des Partnernetzwerks und auf der Registerkarte **Ausgehende Partnernetzwerk-Informationen** wird nicht mehr angezeigt. Der Status der ausgehenden Partnernetzwerk-Informationen wird auf **Versendet** gesetzt.

Nachdem die Partnernetzwerk-Informationen über den MFTP-Kanal an das Partnernetzwerk zugestellt wurden, sendet der ViPNet Network Manager des Partnernetzwerks eine entsprechende Empfangsbestätigung. Der Status der Partnernetzwerk-Informationen auf der Registerkarte **Ausgehende Partnernetzwerk-Informationen** wird von **Versendet** auf **Zugestellt** gesetzt.

Empfang von Änderungen der Partnernetzwerk-Informationen aus einem anderen ViPNet Netzwerk

Wenn der Administrator eines Partnernetzwerks Änderungen an seinem Netzwerk vornimmt, sollte er die aktualisierten Partnernetzwerk-Informationen über einen geschützten Verbindungskanal an Ihr Netzwerk weiterleiten.

Nachdem die Partnernetzwerk-Information aus dem Partnernetzwerk an Ihr Netzwerk zugestellt wurden, wird vom Programm ViPNet Network Manager eine Meldung über den Erhalt nicht bearbeiteter Partnernetzwerk-Informationen eingeblendet. Damit die Änderungen auf den Knoten Ihres Netzwerks in Kraft treten, sollten die empfangenen Änderungen der Partnernetzwerk-Informationen angenommen und bearbeitet werden.

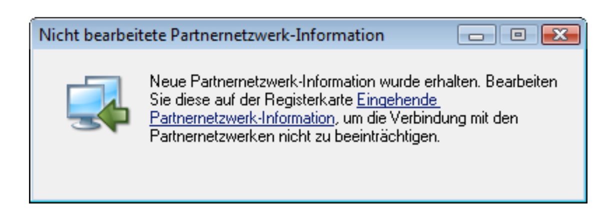


Abbildung 92. Nachricht über eingegangene Partnernetzwerk-Informationen

Klicken Sie im Fenster mit der Meldung auf den Link **Eingehende Partnernetzwerk-Information**. Die Registerkarte **Eingehende Partnernetzwerk-Information** im Bereich **Partnernetzwerke** wird geöffnet. Neben dem Titel der Registerkarte wird das Symbol der unbearbeiteten Partnernetzwerk-Informationen angezeigt. Dieses Symbol wird auch in der Navigationsleiste neben dem Namen des geänderten Partnernetzwerks angezeigt.



Achtung! Stellen Sie sicher, dass auf dem Manager-Arbeitsplatz das Programm ViPNet Monitor gestartet ist. Dieses Programm startet regelmäßig das ViPNet MFTP-Modul, das den Versand von Aktualisierungen durchführt.

Zum Verarbeiten einer Aktualisierung der Partnernetzwerk-Informationen:

1 Wählen Sie in der Navigationsleiste den Knoten **Partnernetzwerke**.

2 Öffnen Sie in der Panel-Ansicht die Registerkarte **Eingehende Partnernetzwerk-Information**.

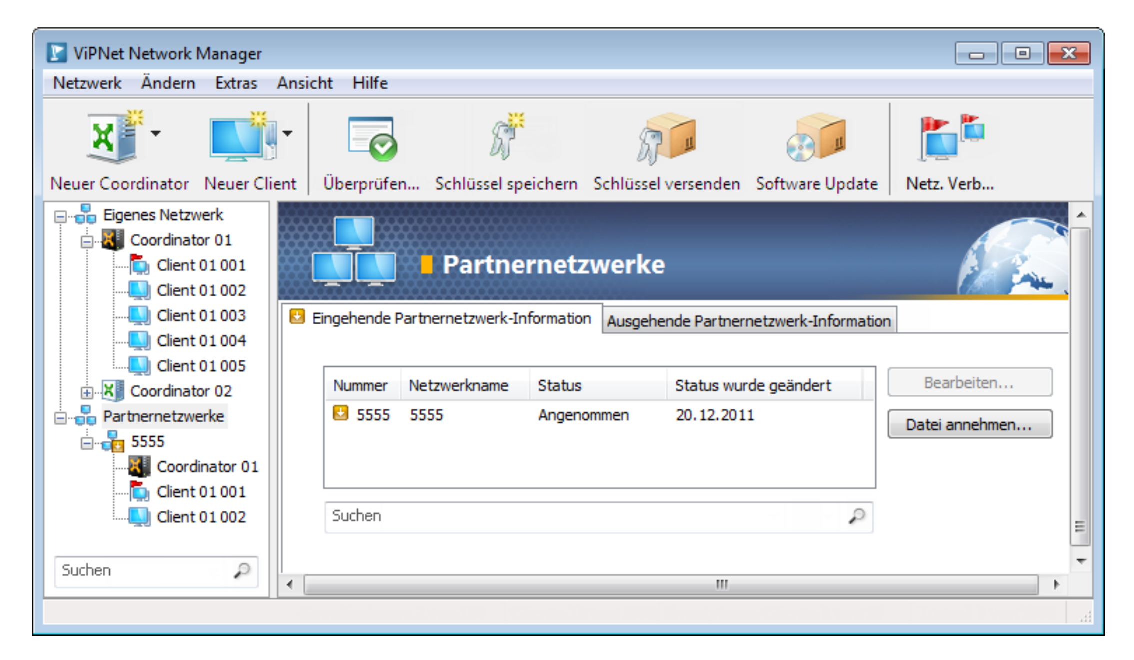


Abbildung 93. Eingehende Partnernetzwerk-Informationen

3 Wählen Sie in der Liste die Zeile mit der eingehenden Partnernetzwerk-Information aus, die mit dem Symbol gekennzeichnet ist. Der Status der eingehenden Partnernetzwerk-Information sollte **Nicht bearbeitet** lauten. Klicken Sie auf **Bearbeiten**.



Hinweis. Wenn aktualisierte Partnernetzwerk-Informationen nicht über das MFTP-Modul zugestellt werden können, kann dazu eine Datei verwendet werden, die vom Administrator des Partnernetzwerks übergeben wird.

Klicken Sie auf **Datei annehmen**, um die erhaltene Datei mit Partnernetzwerk-Informationen zu verarbeiten und folgen dann den Anweisungen, die im Abschnitt Annahme und Verarbeitung von Partnernetzwerk-Informationen (auf S. 171) aufgelistet wird.

4 Machen Sie sich auf der Seite **Partnernetzwerk-Informationen wurden vom Administrator des anderen ViPNet Netzwerks geändert** mit den Änderungen vertraut, die der Administrator des Partnernetzwerks vorgenommen hat.

- Wenn die Partnernetzwerk-Informationen keine neuen oder geänderten Verbindungen zwischen den Netzwerkknoten beider Netzwerke enthalten:

- Klicken Sie auf **Annehmen**, um die Bearbeitung der Partnernetzwerk-Information abzuschließen.
- Klicken Sie auf **Ablehnen**, und dann im eingeblendeten Fenster zur Bestätigung auf **Ja**, um die Änderungen abzulehnen. Der Assistent zur Verwaltung von Partnernetzwerk-Verbindungen wird beendet, der Status der Partnernetzwerk-Informationen ändert sich auf **Abgelehnt**, das Symbol wird nicht mehr angezeigt. Anschließend können die Gründe für die Ablehnung dem Administrator des Partnernetzwerks mitgeteilt und neue Partnernetzwerk-Informationen angefordert werden.
- Wenn Sie eine Entscheidung später treffen möchten, schließen Sie den Assistenten **Partnernetzwerk-Verbindung**.

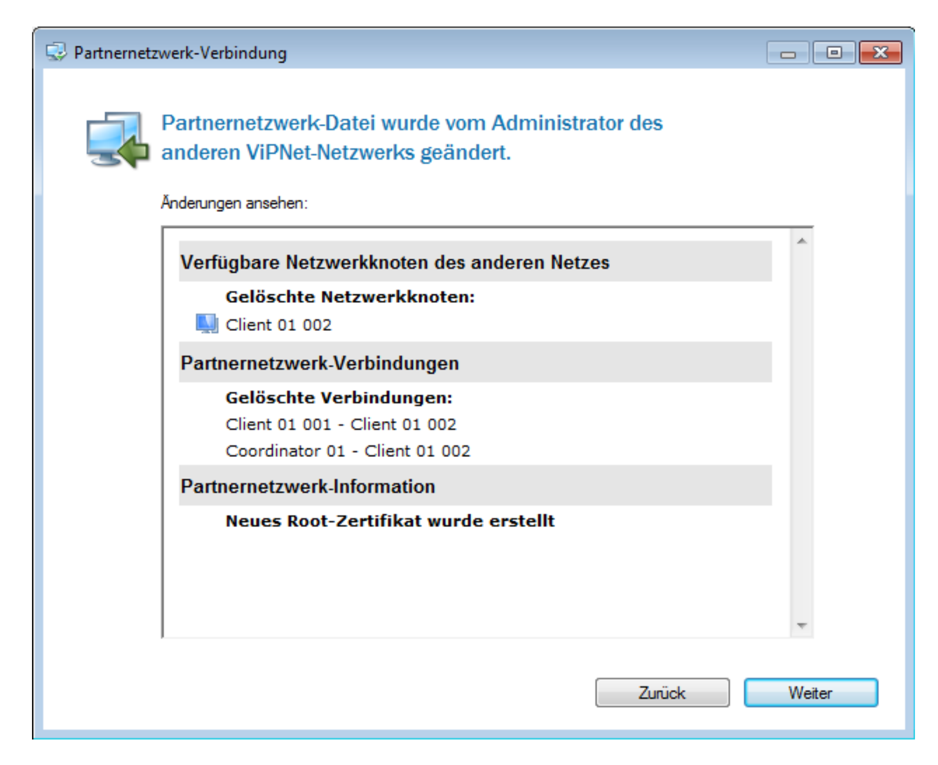


Abbildung 94. Partnernetzwerk-Information enthält keine neuen Verbindungen

- Wenn der Administrator des Partnernetzwerks neue Verbindungen zu den Netzwerkknoten Ihres Netzwerks hinzugefügt hat, klicken Sie auf **Weiter**.

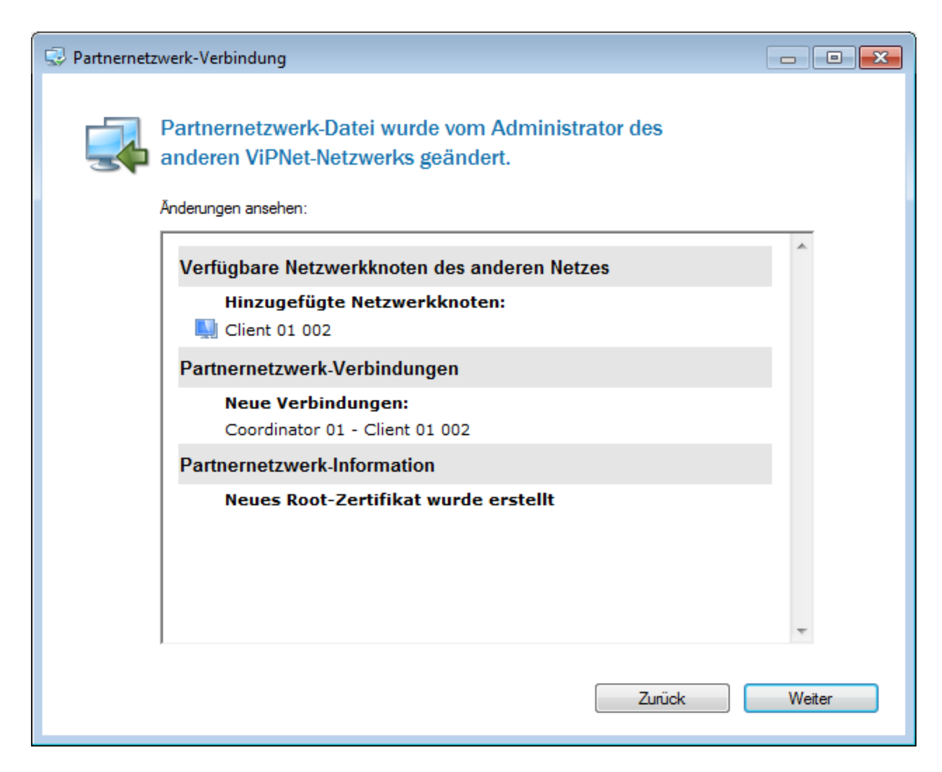


Abbildung 95. Partnernetzwerk-Information enthält neue Verbindungen

Die Seite **Verbindungen mit anderen ViPNet Netzwerken** wird geöffnet. Bearbeiten Sie bei Bedarf die Verbindungen zwischen den Knoten des eigenen und des Partnernetzwerks.

Klicken Sie auf **Annehmen**, um die Bearbeitung der Partnernetzwerk-Information abzuschließen. Klicken Sie auf **Ablehnen**, um die Änderungen abzulehnen.

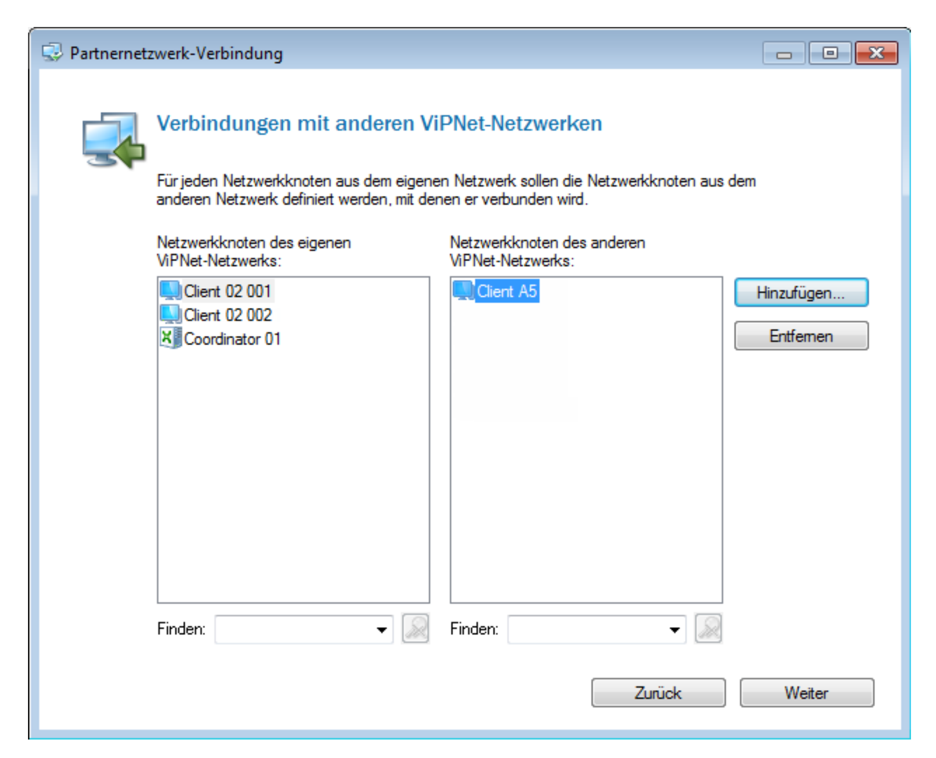


Abbildung 96. Verbindungen mit anderen ViPNet-Netzwerkknoten bearbeiten

Aktivieren Sie auf der Seite **Partnernetzwerk-Informationen werden bearbeitet** das Kontrollkästchen **Schlüsseldistribution erstellen und senden (empfohlen)**. Die Schlüsseldistributionen können auch später erstellt und versendet werden. Dann werden die Änderungen in den Partnernetzwerk-Informationen auf den Netzwerkknoten Ihres Netzwerks erst nach dem Versand der Schlüsseldistributionen übernommen.

Klicken Sie auf **Fertig**.

Wenn die Partnernetzwerk-Informationen angenommen wurden, treten die Änderungen nun in Kraft. Das Symbol der eingehenden Partnernetzwerk-Informationen neben dem Namen des Partnernetzwerks wird nicht mehr angezeigt. Auf der Registerkarte **Ausgehende Partnernetzwerk-Information** wird der Status der Partnernetzwerk-Informationen auf **Bearbeitet** gesetzt.

Deaktivieren der Partnernetzwerk-Kommunikation

Bei Bedarf kann die Kommunikation mit dem Partnernetzwerk wieder eingestellt werden. In diesem Fall werden die Knoten Ihres Netzwerks keine Verbindungen mehr zu Knoten des Partnernetzwerks herstellen können.

Zum Deaktivieren von Partnernetzwerk-Verbindungen:

1 Wählen Sie in der Navigationsleiste das Partnernetzwerk aus, zu dem keine Verbindungen mehr hergestellt werden sollen.

2 Wählen Sie im Menü **Ändern** den Eintrag **Löschen** oder drücken die **Entf**-Taste.

3 Klicken Sie im Bestätigungsfenster auf **Ja**. Wenn die Partnernetzwerk-Verbindungen nicht deaktiviert werden sollen, klicken Sie auf **Nein**.

4 Nach der Bestätigung werden alle Daten des Partnernetzwerks gelöscht. In der Navigationsleiste wird das Symbol dieses Partnernetzwerks nicht mehr angezeigt.



Hinweis. Wenn die Deaktivierung von Partnernetzwerk-Verbindungen wieder rückgängig gemacht werden soll, stellen Sie sofort nach dem Löschen der Partnernetzwerkdaten die letzte gesicherte Konfiguration von ViPNet Network Manager (s. Wiederherstellen der Konfiguration auf S. 155) wieder her.

8

Konfiguration von IPsec-Verbindungen mit mobilen Geräten und anderen Netzwerken

IPsec-Verbindung zu anderen Netzwerken

Das Programm ViPNet Network Manager ermöglicht es, die Interaktion zwischen dem ViPNet Netzwerk und anderen Netzwerken, in denen keine ViPNet Software verwendet wird, über IPsec zu konfigurieren. Als IPsec-Gateway auf der Seite des ViPNet Netzwerks tritt der ViPNet Coordinator HW/VA-Coordinator auf. Beim Weiterleiten des Traffics aus dem ViPNet Netzwerk zu einem Remotenetzwerk entschlüsselt der Coordinator die Pakete des ViPNet Netzwerks und verschlüsselt diese dann nach der IPsec-Technologie. Innerhalb des Remotenetzwerks (vom Remote-IPsec-Gateway bis zu den Endknoten) wird der Traffic offen übertragen. Beim Eintreffen des Traffics aus dem Remotenetzwerk entschlüsselt der Coordinator wiederum die IPsec-Pakete und verschlüsselt sie gemäß der ViPNet Technologie vor der Weiterleitung an die ViPNet Netzwerkknoten.



Abbildung 97. Interaktion zwischen ViPNet-Netzwerk und anderen Netzwerken über die IPsec-Technologie

Führen Sie die folgenden Schritte aus, um IPsec-Verbindungen zu einem anderen Netzwerk im Programm ViPNet Network Manager zu konfigurieren:

1 Wählen Sie im Hauptfenster in der Navigationsleiste den ViPNet Coordinator HW/VA aus, der als IPsec-Gateway auf der Seite des ViPNet Netzwerks auftreten soll.

2 Stellen Sie sicher, dass alle Netzwerkknoten-Parameter korrekt eingestellt sind (s. Konfiguration der Coordinatoren auf S. 109).

3 Öffnen Sie in der Panel-Ansicht die Registerkarte **IPsec-Verbindung**.

4 Aktivieren Sie in der Registerkarte **IPsec-Verbindung** das Kontrollkästchen **Coordinator für geschützte IPsec-Verbindung anderer Netzwerke verwenden**.

5 Wählen Sie in der Liste **Netzwerkadapter-Name** den Netzwerkadapter des Coordinators aus, der für IPsec-Verbindungen verwendet werden soll.

6 Geben Sie im Feld **IP-Adresse oder DNS-Name des Gateways** die öffentliche IP-Adresse oder den DNS-Namen ein, über welche eine Verbindung zum Coordinator aus dem Internet hergestellt werden kann.



Hinweis. Wenn der Coordinator über keine statische IP-Adresse verfügt, kann für ihn ein DNS-Name mit Hilfe des dynamischen DNS-Dienstes registriert werden.

7 Klicken Sie auf die Schaltfläche **Hinzufügen**.

Es wird das Fenster **Neues IPsec-Gateway** geöffnet.

8 Geben Sie in der Registerkarte **Verbindung** die folgenden Parameter an:

- **Remotegateway-Name**: Name des IPsec-Gateways des Remotenetzwerks.
- **Remotegateway-IP-Adresse**: IP-Adresse des IPsec-Gateways des Remotenetzwerks.
- **IP-Adresse des lokalen Netzwerks**: IP-Adressen der Knoten des eigenen Netzwerks und der Knoten des Remotenetzwerks, zwischen denen IPsec-Verbindungen möglich sein sollen. Klicken Sie auf die Schaltfläche **Hinzufügen** und geben im Fenster **Adressen des lokalen und Remotenetzwerks** die IP-Adressen der Knoten an.

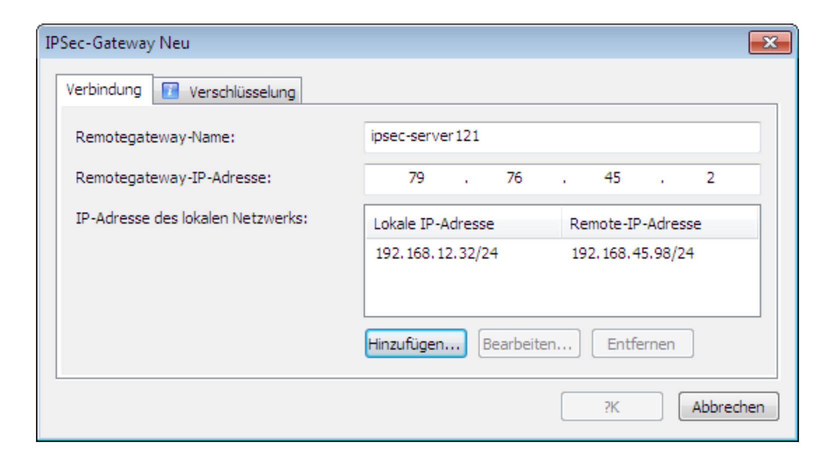


Abbildung 98. Angeben der Parameter für remote IPsec-Gateway

9 Geben Sie in der Registerkarte Verschlüsselung die folgenden Parameter an:

- **Pre-Shared Key**: eine beliebige Reihenfolge von Zeichen (nicht mehr als 256), die zur Überprüfung der Authentizität der Verbindung verwendet wird.
- **Verschlüsselungsalgorithmus**: Algorithmus zur Verschlüsselung von Daten, die über IPsec übertragen werden. Dazu gehören **3des** (standardmäßig eingestellt) und **aes**. Der Algorithmus AES gilt als der widerstandsfähigere der beiden Algorithmen.
- **Hashalgorithmus**: Algorithmus zum Hashing von Daten (standardmäßig ist **sha1** ausgewählt). Unter den verfügbaren Algorithmen gilt der Algorithmus SHA1 als der mit der höchsten, der Algorithmus MD5 als der mit der niedrigsten Widerstandsfähigkeit.
- **Diffie-Hellman-Parameter**: kryptografischer Parameter des Diffie-Hellman-Algorithmus zur Erstellung des Sitzungsschlüssels. Der Wert des Parameters ist proportional zur Stärke der Verschlüsselung. Für ViPNet Software beträgt der Standardwert **2**.
- **Schlüsselgültigkeitsdauer (in Stunden)**: die Gültigkeitsdauer der Sitzungsschlüssel (in Stunden), die die Länge einer Sitzung für den Datenaustausch festlegt. Der Wert dieses Parameters hängt von der verwendeten Software ab. Für ViPNet Software beträgt der Standardwert **8**.

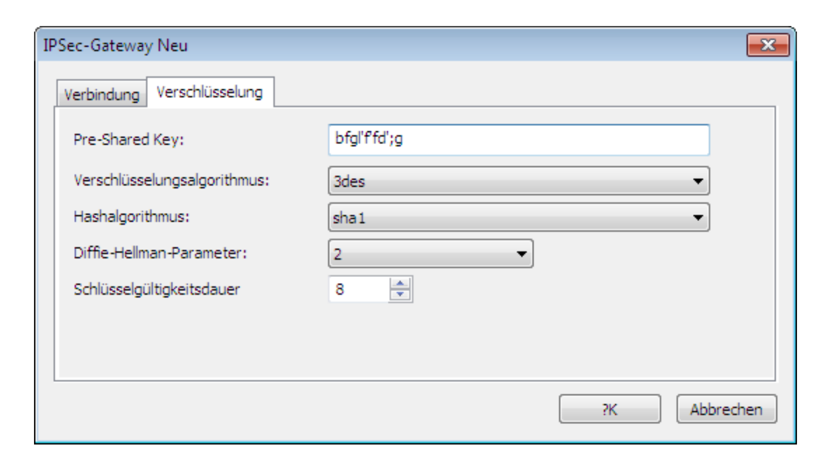


Abbildung 99. Definition der Verschlüsselungsparameter



Achtung! Die Werte der Verschlüsselungsparameter sollten in den beiden miteinander kommunizierenden Netzwerken übereinstimmen. Demgemäß sind sie das Ergebnis einer gegenseitigen Absprache zwischen den Administratoren der betroffenen Netzwerke.

10 Klicken Sie auf **OK**.

11 Klicken Sie in der Panel-Ansicht in der Registerkarte **Schlüssel** auf die Schaltfläche **Schlüssel senden**, um die IPsec-Verbindungseinstellungen an den ViPNet Coordinator HW/VA zu übermitteln.

Wenn auf dem ViPNet Coordinator HW/VA keine Schlüssel installiert sind, klicken Sie auf **Schlüssel speichern** (s. Speichern der Schlüsseldistributionen auf S. 142), um die Schlüssel zu erstellen. Übergeben Sie anschließend die Schlüssel zusammen mit der Konfigurationsdatei `hwinit_set.xml` dem Administrator des Coordinators.

12 Konfigurieren Sie auf dem ViPNet Coordinator HW/VA-Knoten einen Transitfilter des offenen Netzwerks, der den Traffic der Remote-Netzwerkknoten in Richtung der lokalen Netzwerkknoten erlaubt. Details s. Dokument „ViPNet Coordinator HW/VA. Referenzhandbuch“.



Hinweis. Damit die Knoten des Remote-Netzwerks die Möglichkeit haben, Verbindungen zu geschützten ViPNet Knoten in Ihrem lokalen Netzwerk aufzubauen, sollten Filter des offenen Netzwerks (s. Allgemeine Informationen über Netzwerkfilter auf S. 274) auf den geschützten ViPNet Knoten konfiguriert werden, die solche Verbindungen erlauben.

Nachdem die vorgenommenen Einstellungen auf dem ViPNet Coordinator HW/VA angewendet wurden, können Daten mit dem Remotenetzwerk über die IPsec-Technologie ausgetauscht werden.

Anbindung mobiler Geräte an das ViPNet Netzwerk

Moderne Geschäftsprozesse sehen einen aktiven Einsatz mobiler Endgeräte vor. Mit Hilfe von mobilen Geräten können Mitarbeiter, die sich nicht an ihren Arbeitsplätzen befinden, das betriebliche E-Mail-System, die Möglichkeiten der IP-Telefonie oder andere Ressourcen des Firmennetzwerks nutzen.

Für den geschützten Zugang zu unternehmensinternen Ressourcen innerhalb des ViPNet Netzwerks können mobile Geräte (Smartphones) unterschiedlicher Typen verwendet werden. Der Schutz des Traffics wird dabei mit Hilfe einer Kombination der IPsec- und der ViPNet Technologie sichergestellt. Die Parameter der Anbindung von Smartphone-Clients mit Betriebssystem iOS an das ViPNet Netzwerk können im Programm ViPNet Network Manager konfiguriert werden. Dabei sind keine zusätzlichen Einstellungen auf den Geräten selbst erforderlich. Die ViPNet Netzwerkverbindungseinstellungen für mobile Geräte mit Betriebssystem Android können ebenfalls in ViPNet Network Manager konfiguriert werden. Diese Einstellungen werden jedoch nur auf den Coordinator angewendet. Auf dem mobilen Gerät selbst sollten die Einstellungen manuell konfiguriert werden.



Abbildung 100. Das Prinzip der Anbindung eines Geräts an das ViPNet-Netzwerk

Die Verbindung zwischen dem offenen Netzwerkknoten und dem ViPNet Knoten erfolgt mit Hilfe des Coordinators, der die Rolle des Gateways ViPNet – IPsec übernimmt. Der offene Knoten verbindet sich mit dem Coordinator über die IPsec-Technologie. Dabei wird ein verschlüsselter Tunnel vom offenen Knoten zum Coordinator aufgebaut. Dem offenen Knoten wird auf dem Coordinator eine IP-Adresse aus einem vorgegebenen Bereich (in der Abbildung 10.0.0.5) zugeordnet.

Auf dem Coordinator wird die Tunnelung des IP-Adressenbereichs, der die mobilen Endgeräte umfasst, mit Hilfe der ViPNet Technologie verwirklicht. Geschützte ViPNet Knoten, die mit dem Coordinator verbunden sind, sind für die mobilen Geräte über sichtbare Adressen auf dem Coordinator erreichbar (in der Abbildung 192.168.2.10). Wenn der Zugriff mobiler Endgeräte auf ViPNet Knoten über DNS-Namen erfolgen soll, muss auf dem Coordinator, der die Rolle des IPsec-Gateways übernimmt, ein DNS-Server konfiguriert werden (s. DNS- bzw. WINS-Server auf dem geschützten oder getunnelten Knoten auf S. 307).

IP-Pakete, die vom mobilen Endgerät über IPsec-Technologie versendet wurden, werden vom Coordinator entschlüsselt, anschließend vom ViPNet Treiber wieder verschlüsselt und über das

geschützte ViPNet Netzwerk an den benötigten Netzwerkknoten weitergeleitet. In gleicher Weise werden IP-Pakete in entgegengesetzter Richtung übertragen.



Hinweis. Wenn die Anwendungsserver oder andere Objekte, die vom mobilen Gerät aus erreichbar sein sollen, sich unmittelbar auf dem Coordinator befinden, der die Rolle eines IPsec-Gateways übernimmt, dann ist eine Konfiguration der Tunnelung mobiler Endgeräte nicht notwendig.

Der Coordinator, der die Rolle eines IPsec-Gateways übernimmt, muss folgende Anforderungen erfüllen:

- Coordinator einer der folgenden Typen:
  - ViPNet Coordinator HW/VA-Coordinator (s. Verwendung eines ViPNet Coordinator HW/VA als IPsec-Gateway für Anbindung mobiler Endgeräte auf S. 207).
  - Windows-Coordinator mit dem Betriebsystem Windows Server 2008 R2 (s. Verwendung eines Windows-Coordinators als IPsec-Gateway für Anbindung mobiler Endgeräte auf S. 193).



Hinweis. Die Funktionen des IPsec-Gateways kann auch ein Computer mit dem Betriebssystem Windows Server 2003 übernehmen. Die in diesem Dokument enthaltenen Hinweise zur Konfiguration des IPsec-Gateways beziehen sich allerdings auf das Betriebssystem Windows Server 2008 R2.

Wenden Sie sich an den technischen Kundendienst von Infotecs GmbH, falls Sie Hilfe beim Konfigurieren des IPsec-Gateways unter Windows Server 2003 benötigen.

- Der Coordinator muss vom Internet aus über eine feste IP-Adresse oder einen DNS-Namen erreichbar sein (der Name kann mit Hilfe eines dynamischen DNS-Dienstes registriert werden).

Verwendung eines Windows-Coordinators als IPsec-Gateway für Anbindung mobiler Endgeräte

Damit Verbindungen mobiler Geräte zum ViPNet Netzwerk mit Hilfe des Windows-Coordinators sichergestellt werden können, müssen auf dem ViPNet Coordinator zunächst ein IPsec-Gateway eingerichtet sowie IPsec-Profile für Smartphone-Clients erstellt und installiert werden.

Vorgehensweise bei Anbindung von Smartphone-Clients an das ViPNet Netzwerk

Führen Sie die in der unteren Tabelle aufgeführten Schritte aus, um einen neuen IPsec-Gateway einzurichten und um Smartphone-Clients an diesen Server anzubinden.

Tabelle 10. Neuen IPsec-Gateway und Smartphone-Clients hinzufügen

	Aktion	**Verweis**
☐	Wählen oder erstellen Sie im Programm ViPNet Network Manager einen Coordinator, der die Rolle des IPsec-Gateways übernehmen soll, und konfigurieren die Verbindungsparameter über das IPsec-Protokoll.	Konfiguration des IPsec-Profils für den Windows-Coordinator (auf S. 195)
☐	Wenn der Zugang mobiler Geräte zu geschützten ViPNet Knoten bereitgestellt werden soll, dann definieren bei der Konfiguration des IPsec-Gateways einen Bereich getunnelter IP-Adressen für die Smartphone-Clients.	Konfiguration des IPsec-Profils für den Windows-Coordinator (auf S. 195) Tunnelung (auf S. 114)
☐	Fügen Sie auf dem Coordinator die benötigte Anzahl an Smartphone-Clients hinzu und konfigurieren ihre Parameter.	Profile IPsec für Smartphone-Clients einstellen (auf S. 211)
☐	Konfigurieren Sie das IPsec-Profil für den Coordinator.	Konfiguration des IPsec-Profils für den Windows-Coordinator (auf S. 195)
☐	Fügen Sie auf dem Coordinator die Rolle „Netzwerkrichtlinien und Zugriffsdienste" hinzu und starten den Routing- und RAS-Dienst.	Hinzufügen der Rolle „Netzwerkrichtlinien- und Zugriffsdienste" in Windows Server 2008 R2 (auf S. 197) Starten des Routing- und RAS-Dienstes (auf S. 199)

	Aktion	Verweis
☐	Wenden Sie auf dem Coordinator das früher erstellte IPsec-Profil an.	Anwenden des IPsec-Profils auf dem Windows-Coordinator (auf S. 200)
☐	Konfigurieren Sie auf dem Coordinator ein Filter des offenen Netzwerks, welcher die Verbindungen mobiler Geräte über das IPsec-Protokoll erlaubt.	Konfiguration von Filter des offenen Netzwerks auf dem Coordinator (auf S. 201)
☐	Wenn der Coordinator über eine Firewall mit dem Internet verbunden ist, konfigurieren Sie auf dieser Firewall die Regeln für die Weiterleitung von IP-Paketen des IPsec-Protokolls.	Konfiguration von Regeln für die externe Firewall (auf S. 203)
☐	Wenn der Zugriff mobiler Clients auf die Ressourcen unmittelbar auf dem Coordinators ermöglicht werden soll, dann konfigurieren lokaler Filter des offenen Netzwerks für die Weiterleitung des Traffics über entsprechende Protokolle und Ports.	Konfiguration von Filter für den Zugang von Smartphone-Clients zu Objekten auf dem Coordinator (auf S. 204)
☐	Konfigurieren Sie auf dem Coordinator ein Filter und die Regel der Adressenübersetzung, um den Zugang mobiler Geräte zum Internet zu gewährleisten.	Konfiguration von Filter und NAT-Regel für den Zugang von Smartphone-Clients zum Internet (auf S. 205)
☐	Wenn der Zugriff mobiler Geräte auf ViPNet Netzwerkknoten über DNS-Namen erfolgen soll, installieren und konfigurieren Sie auf dem Coordinator einen DNS-Server und registrieren dort die DNS-Namen von ViPNet Netzwerkknoten.	Konfiguration und Verwendung der Namensdienste DNS und WINS im ViPNet Netzwerk (auf S. 305)
☐	Installieren Sie die IPsec-Profile auf den mobilen Apple-Geräten.	Konfiguration mobiler Geräte von Apple (auf S. 213)
☐	Benutzen Sie die mobilen Endgeräte für den Zugriff auf geschützte ViPNet Netzwerkobjekte.	Konfiguration mobiler Geräte von Apple (auf S. 213)

Führen Sie die nachfolgend aufgezählten Aktionen aus, um Smartphone-Clients für die Anbindung an einen bestehenden IPsec-Coordinator hinzuzufügen.

Tabelle 11. Mobile Clients auf einem bestehenden IPsec-Gateway hinzufügen

	Aktion	Verweis
☐	Fügen Sie auf dem bestehenden IPsec-Coordinator die benötigte Anzahl an mobilen Clients hinzu und konfigurieren ihre Parameter.	Profile IPsec für Smartphone-Clients einstellen (auf S. 211)
☐	Wenn nötig, erhöhen Sie die Anzahl der IP-Adressen und Verbindungen, die vom Coordinator getunnelt werden.	Tunnelung (auf S. 114)
☐	Konfigurieren Sie das IPsec-Profil für den Coordinator.	Konfiguration des IPsec-Profils für den Windows-Coordinator (auf S. 195)
☐	Wenden Sie das zuvor gespeicherte IPsec-Profil auf	Anwenden des IPsec-Profils auf dem

	Aktion	Verweis
	dem Coordinator an.	Windows-Coordinator (auf S. 200)
☐	Installieren Sie die IPsec-Profile auf den neuen mobilen Apple-Geräten.	Konfiguration mobiler Geräte von Apple (auf S. 213)
☐	Benutzen Sie die neu hinzugefügten mobilen Endgeräte für den Zugriff auf geschützte ViPNet Netzwerkobjekte.	Konfiguration mobiler Geräte von Apple (auf S. 213)

Konfiguration des IPsec-Profils für den Windows-Coordinator

Als IPsec-Gateway kann ein Coordinator eingesetzt werden, der unter der Verwaltung des Betriebssystems Windows Server 2008 R2 läuft.

Führen Sie die folgenden Schritte aus, um das Profil des IPsec-Gateways einzustellen:

1 Wählen Sie im Programm ViPNet Network Manager in der Navigationsleiste den Coordinator ViPNet Coordinator Windows aus, der als IPsec-Gateway auftreten soll.

2 Öffnen Sie in der Panel-Ansicht die Registerkarte **IPsec-Verbindung**.



Abbildung 101. IPsec-Verbindungsparameter für Windows-Coordinator einstellen



Hinweis. Die Registerkarte **IPsec-Verbindung** wird nur dann eingeblendet, wenn eine Lizenz für den Einsatz des Coordinators als IPsec-Gateway vorliegt. Wenn alle vorhandenen Lizenzen aufgebraucht sind, ist die Konfiguration der Parameter in dieser Registerkarte nicht möglich.

3 Damit auf dem Coordinator ein IPsec-Profil konfiguriert werden kann sowie Smartphone-Clients hinzugefügt werden können, aktivieren Sie das Kontrollkästchen **Coordinator als IPsec-Gateway für Anbindung von Smartphone-Clients verwenden**.



Achtung! Wenn der Coordinator für den Einsatz als IPsec-Gateway bereits konfiguriert ist, werden beim Deaktivieren dieses Kontrollkästchens alle IPsec-Parameter und alle neu hinzugefügten mobilen Clients wieder gelöscht.

4 Geben Sie im Feld **IP-Adresse oder DNS-Name des Gateways** die öffentliche IP-Adresse oder den DNS-Namen ein, über welche eine Verbindung zum Coordinator aus dem Internet hergestellt werden kann.



Hinweis. Wenn der Coordinator über keine statische IP-Adresse verfügt, kann für ihn ein DNS-Name mit Hilfe des dynamischen DNS-Dienstes registriert werden.

5 Geben Sie im Feld **Pre-Shared Key** eine beliebige Reihenfolge an Zeichen ein (nicht mehr als 256). Diese Zeichenfolge wird für die Überprüfung der Verbindungsauthentizität verwendet.

6 Wenn der Zugriff von Smartphone-Clients auf geschützte ViPNet Clients sichergestellt werden soll, konfigurieren Sie zunächst eine Tunnelung dieser Geräte durch den Coordinator. Geben Sie dazu in der Registerkarte **Tunnel** des entsprechenden Coordinators (s. Tunnelung auf S. 114) den IP-Adressenbereich für die Smartphone-Clients sowie die maximal zulässige Anzahl an gleichzeitig getunnelten Verbindungen an.

Adressen, die in der Registerkarte **Tunnel** definiert sind, werden gemeinsam mit dem IPsec-Profil an den Coordinator weitergeleitet. Beim Aufbau einer Verbindung zum Coordinator erhält der Smartphone-Client eine IP-Adresse aus dem angegebenen Bereich. Zusätzlich werden diese Adressen als getunnelte Adressen auf dem Coordinator geführt.



Achtung! Die Anzahl getunnelter IP-Adressen des Coordinators muss die Anzahl der Smartphone-Clients, die sich voraussichtlich zu diesem Coordinator verbinden werden, mindestens um eins übersteigen.

7 Fügen Sie auf dem Coordinator die benötigte Anzahl an Smartphone-Clients hinzu und konfigurieren ihre Parameter (s. Profile IPsec für Smartphone-Clients einstellen auf S. 211).

8 Nachdem Sie die erforderlichen Einstellungen für den Coordinator und die Smartphone-Clients vorgenommen haben, klicken Sie in der Registerkarte **IPsec-Verbindung** auf die Schaltfläche **IPsec-Profil speichern**.

Geben Sie im Fenster **Ordner auswählen** den Ordner an, in welchem die Profildateien abgelegt werden sollen.

9 Im angegebenen Ordner werden die Dateien `run.bat` und `createuser.vbs` erstellt. Verwenden Sie diese Dateien dazu, die vordefinierten IPsec-Parameter auf dem Coordinator anzuwenden (s. Anwenden des IPsec-Profils auf dem Windows-Coordinator auf S. 200).

Konfiguration des IPsec-Gateways

In diesem Abschnitt wird die Konfiguration eines Coordinators beschrieben, der unter der Steuerung des Betriebssystems Windows arbeitet und als IPsec-Gateway eingesetzt wird.

Hinzufügen der Rolle „Netzwerkrichtlinien- und Zugriffsdienste" in Windows Server 2008 R2

Wenn der Server, der für die Anbindung von Apple-Geräten an das ViPNet Netzwerk konfiguriert werden soll, ein Teil der Domäne ist, dann stellen Sie sicher, dass dieser Server vom Administrator in Gruppe RAS und IAS-Server hinzugefügt wurde. Führen Sie dazu die folgenden Schritte durch:

1 Melden Sie sich auf dem Server mit dem Konto des Domänenadministrators an.

2 Öffnen Sie das Snap-In „Active Directory-Benutzer und -Computer".

3 Doppelklicken Sie im Bereich **Benutzer** auf die Gruppe **RAS- und IAS-Server**.

4 Stellen Sie sicher, dass im Fenster der Gruppeneigenschaften in der Registerkarte **Mitglieder** der Server eingetragen ist, der konfiguriert werden soll. Wenn nötig, fügen Sie den Server in dieser Gruppe hinzu.

Führen Sie folgende Schritte aus, um die Rolle „Netzwerkrichtlinien- und Zugriffsdienste" im Betriebssystem Windows Server 2008 R2 hinzuzufügen:

1 Zeigen Sie im Menü **Start** auf den Eintrag **Verwaltungsprogramme** und klicken anschließend auf **Server-Manager**.

2 Klicken Sie im Snap-In **Server-Manager** in der linken Leiste mit der rechten Maustaste auf den Eintrag **Rollen** und wählen im Kontextmenü den Punkt **Rollen hinzufügen**.

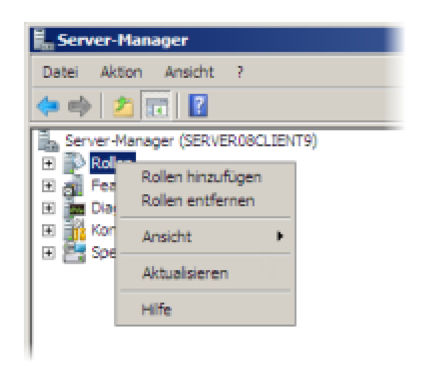


Abbildung 102. Rollen auf dem Server hinzufügen

Es wird der **Assistent zum Hinzufügen von Rollen** gestartet.

3 Klicken Sie auf der ersten Seite des Assistenten auf **Weiter**.

4 Aktivieren Sie auf der Seite **Serverrollen** das Kontrollkästchen **Netzwerkrichtlinien- und Zugriffsdienste** und klicken auf **Weiter**.

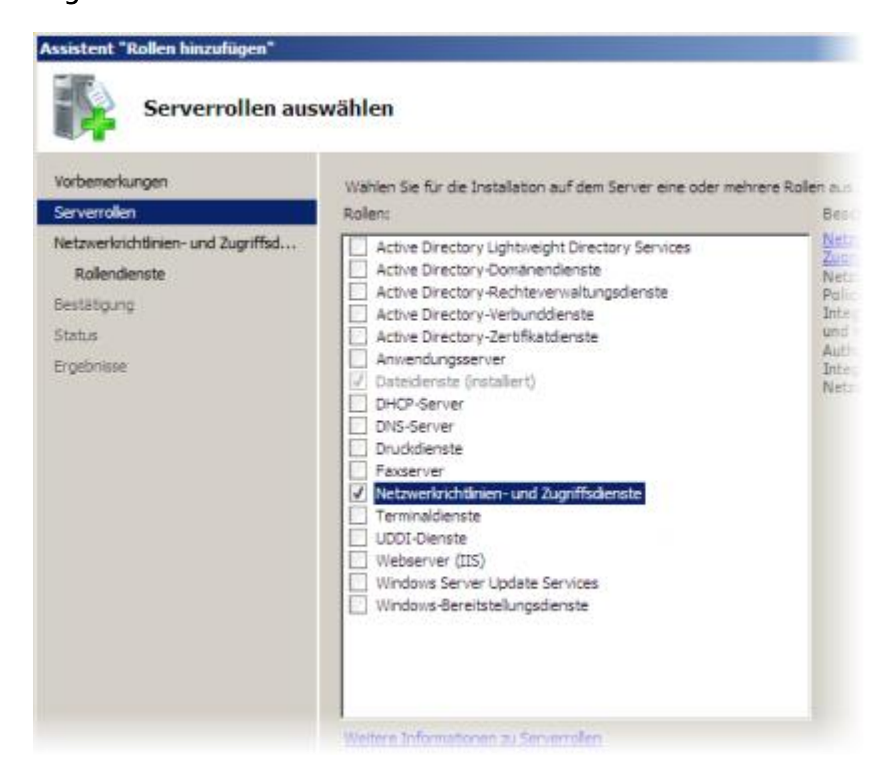


Abbildung 103. Rolle für die Installation auswählen

5 Nehmen Sie auf der nachfolgenden Seite des Assistenten die aufgeführten Informationen zur Kenntnis und klicken auf **Weiter**.

6 Aktivieren Sie auf der Seite **Rollendienste** das Kontrollkästchen **Routing- und RAS-Dienste** (die Einträge **RAS** und **Routing** werden automatisch ausgewählt) und klicken anschließend auf **Weiter**.

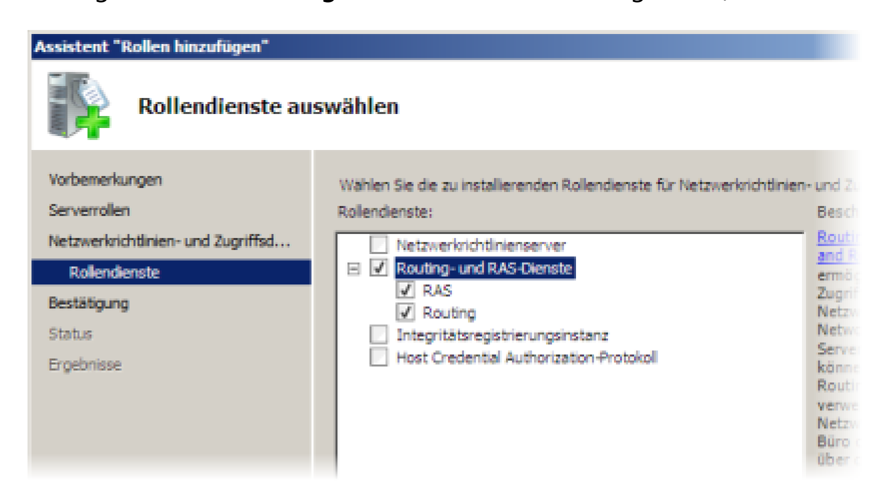


Abbildung 104. Dienste für die Installation auswählen

7 Klicken Sie auf der Seite **Bestätigung** auf **Installieren**. Der Installationsvorgang wird gestartet.

8 Auf der Seite **Installationsstatus** wird der Fortschritt des Installationsvorgangs dargestellt. Nach Abschluss der Installation wird die Seite **Installationsergebnisse** eingeblendet.

9 Klicken Sie auf **Schließen**, um die Installation fertigzustellen.

Die Rolle „Netzwerkrichtlinien- und Zugriffsdienste" und alle benötigten Dienste sind installiert.

Starten des Routing- und RAS-Dienstes

Führen Sie im Betriebssystem Windows Server 2008 R2 die folgenden Schritte aus, um den Routing- und RAS-Dienst auf dem Coordinator zu starten:

1 Wählen Sie im Menü **Start** den Eintrag **Verwaltung** und klicken anschließend auf **Server-Manager**.

2 Klicken Sie im Snap-In **Server-Manager** in der linken Leiste mit der rechten Maustaste auf den Eintrag **Rollen** > **Netzwerkrichtlinien- und Zugriffsdienste** > **Routing und RAS** und wählen im Kontextmenü den Punkt **Routing und RAS konfigurieren und aktivieren**.

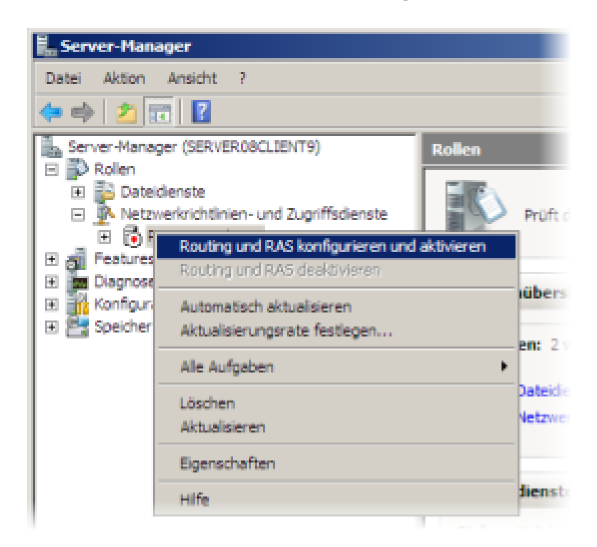


Abbildung 105. Routing- und RAS-Dienst in Windows Server 2008 einstellen

Es wird der **Setup-Assistent für den Routing- und RAS-Server** gestartet.

3 Klicken Sie auf der ersten Seite des Assistenten auf **Weiter**.

4 Wählen Sie auf der Seite **Konfiguration** die Option **RAS (DFÜ oder VPN)** und klicken anschließend auf **Weiter**.



Abbildung 106. Konfiguration auswählen

5 Aktivieren Sie auf der Seite **RAS** das Kontrollkästchen **VPN-Zugriff und NAT** und klicken auf **Weiter**.

6 Wählen Sie auf der Seite **VPN-Verbindung** den Netzwerkadapter aus, der an das Internet angeschlossen ist, und klicken auf **Weiter**.

7 Übernehmen Sie auf den Seiten **IP-Adresszuweisung** und **Mehrere RAS-Server verwalten** die Standarteinstellungen und klicken auf **Weiter**.

8 Klicken Sie auf der letzten Seite des Assistenten auf die Schaltfläche **Fertig stellen**.

Es wird der **Routing- und RAS-Dienst** gestartet.

Anwenden des IPsec-Profils auf dem Windows-Coordinator

Führen Sie die folgenden Schritte aus, um die im Programm ViPNet Network Manager definierten IPsec-Verbindungsparameter auf dem Coordinator anzuwenden:

1 Speichern Sie das IPsec-Profil, das für den Coordinator konfiguriert wurde (s. Konfiguration des IPsec-Profils für den Windows-Coordinator auf S. 195), im Programm ViPNet Network Manager ab und übertragen die angelegten Dateien auf den Coordinator.

2 Starten Sie auf dem Coordinator die Datei `run.bat`.

Beim Ausführen der Datei wird in den Eigenschaften des Routing- und RAS-Dienstes der in ViPNet Network Manager definierte Wert für den Pre-Shared Key der Verbindung gesetzt. Als IP-Adressenbereich für IPsec-Knoten werden Adressen definiert, die in ViPNet Network Manager als getunnelte Adressen für den gegebenen Coordinator konfiguriert wurden.



Hinweis. Wenn für den Coordinator keine getunnelten IP-Adressen definiert wurden, werden die Adressen für Smartphone-Clients, die sich zum Coordinator verbinden, vom DHCP-Server vergeben.

Zusätzlich werden zur Liste lokaler Windows-Benutzer auf dem Coordinator Benutzer hinzugefügt, die für Smartphone-Clients im Programm ViPNet Network Manager neu angelegt wurden (s. Profile IPsec für Smartphone-Clients einstellen auf S. 211).

Konfiguration von Filter des offenen Netzwerks auf dem Coordinator

Damit offene Knoten Verbindungen zum Coordinator über das IPsec-Protokoll herstellen können, muss für diese Knoten ein Filter des offenen Netzwerks eingestellt werden, der den Durchlass von IP-Paketen über die Protokolle ESP und UDP auf Port 500 und 4500 erlaubt.

Führen Sie die folgenden Schritte aus, um ein Filter auf dem Coordinator zu konfigurieren:

1. Wählen Sie in der Navigationsleiste des Fensters des Programms ViPNet Monitor den Bereich **Netzwerkfilter** > **Lokale Filter des offenen Netzwerks** aus.
2. Klicken Sie in der Panel-Ansicht auf **Erstellen**.
3. Legen Sie im geöffneten Fenster im Bereich **Allgemeine Optionen** den Namen und das Verhalten des Filters (Traffic erlauben) fest.
4. Behalten Sie im Bereich **Quellen** den Standardwert **Alle Quellen** bei.
5. Führen Sie im Bereich **Ziele** folgende Aktionen durch:
   - Klicken Sie auf **Hinzufügen** und wählen im Menü den Befehl **Mein ViPNet Knoten**.
   - Aktivieren Sie das Kontrollkästchen **Netzwerkadapter** und geben mit Hilfe der Schaltfläche **Auswählen** den Netzwerkadapter, der direkt an das Internet angeschlossen ist.



Abbildung 107. IP-Adressen für lokale Regel angeben

6. Führen Sie im Bereich **Protokolle** folgende Aktionen durch:
   - Klicken Sie auf **Hinzufügen** und wählen **IP-Protokoll** aus.
   - Wählen Sie im Fenster **Protokollliste** den Protokoll `50 – ESP` aus und klicken auf **OK**.



Abbildung 108. Protokoll auswählen

- Klicken Sie auf **Hinzufügen** und wählen **TCP/UDP-Protokoll** aus.
- Wählen Sie im Fenster **TCP/UDP-Protokoll** aus:
  - **Protokoll**: **UDP**,
  - **Quellport**: **Alle Ports**,
  - **Zielport**: **Portnummer**, wählen Sie den Wert `500-isakmp`.

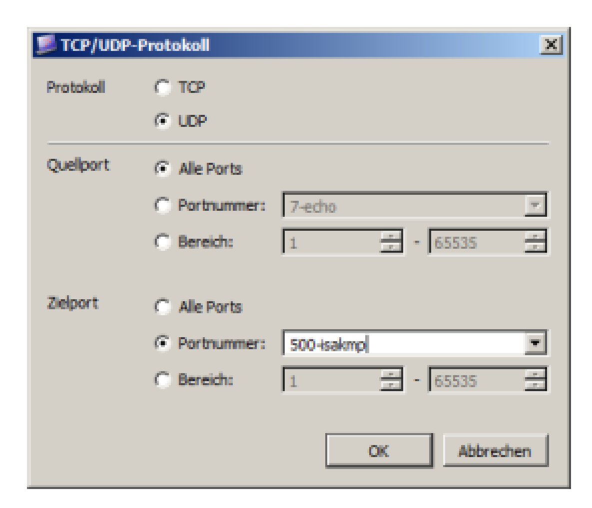


Abbildung 109. Parameter des UDP-Protokolls definieren

- Klicken Sie auf **OK**.
- Klicken Sie auf **Hinzufügen** und wählen **TCP/UDP-Protokoll** aus.
- Wählen Sie im Fenster **TCP/UDP-Protokoll** aus:
  - **Protokoll**: **UDP**,
  - **Quellport**: **Alle Ports**,
  - **Zielport**: **Portnummer**, geben Sie den Wert 4`500` an.
- Klicken Sie auf **OK**.

7 Klicken Sie im Fenster für Optionen des lokalen Filters auf **OK**.

8 Klicken Sie im Bereich **Lokale Filter des offenen Netzwerks** auf **Alle übernehmen**,

Filter, der Verbindungen zum Coordinator über die IPsec-Technologie erlaubt, ist nun konfiguriert.



Abbildung 110. Filter für IPsec-Verbindung

Konfiguration von Regeln für die externe Firewall

Wenn der Coordinator über eine externe Firewall mit dem Internet verbunden ist, sollte auf dieser Firewall (oder DSL-Router) eine Regel für UDP-Pakete konfiguriert werden, die im Zuge der Kommunikation über das IPsec- oder L2TP-Protokoll ausgetauscht werden. Führen Sie dazu eine der folgenden Aktionen aus:

- Stellen Sie sicher, dass auf dem Gerät, das als externe Firewall benutzt wird, die Optionen L2TP Passthrough und IPsec Passthrough aktiviert sind (falls diese Parameter vom entsprechenden Gerät unterstützt werden). Danach sind keine weiteren Aktionen mehr erforderlich.

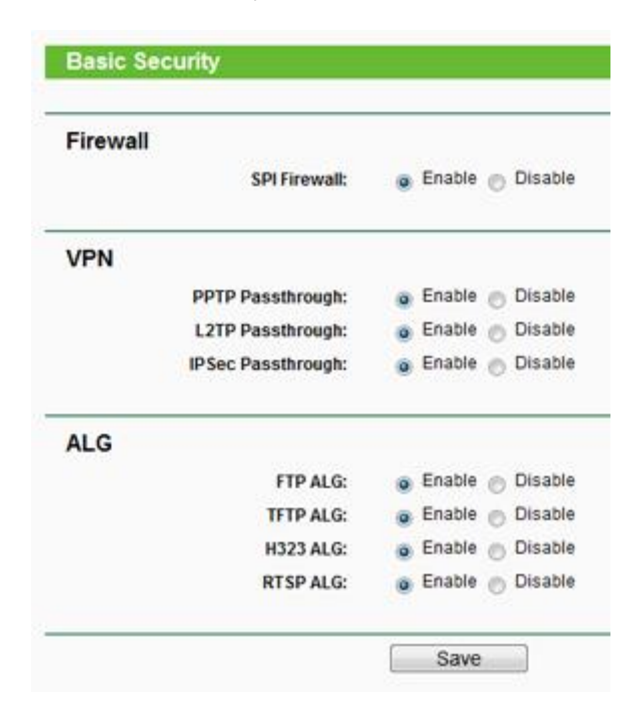


Abbildung 111. Routing-Parameter

- Falls die Parameter L2TP Passthrough und IPsec Passthrough von Ihrem Gerät nicht unterstützt werden, konfigurieren Sie die Regel manuell, indem Sie folgende Parameterwerte verwenden:
  - IP-Adresse des Servers auf dem die Software ViPNet Coordinator installiert ist und zu dem die Portweiterleitung erfolgen soll.
  - Protokoll: UDP. Ports: 500 und 4500.

Konfiguration von Filter für den Zugang von Smartphone-Clients zu Objekten auf dem Coordinator

Wenn der Zugang mobiler Geräte zu Anwendungsservern oder zu anderen Ressourcen auf dem Coordinator sichergestellt werden soll, und der Coordinator dabei als IPsec-Gateway eingesetzt wird, dann muss auf diesem Coordinator lokaler Filter des offenen Netzwerks konfiguriert werden, der Verbindungen über bestimmte Protokolle und Ports erlaubt.

Betrachten wir das Beispiel einer Filter-Konfiguration für Verbindungen zum Webserver, der über Port 80, Protokoll TCP verfügbar ist:

1. Wählen Sie auf dem Coordinator im Programm ViPNet Monitor den Bereich **Netzwerkfilter** > **Lokale Filter des offenen Netzwerk** und erstellen ein neuer lokaler Filter.
2. Klicken Sie in der Panel-Ansicht auf **Erstellen**.
3. Legen Sie im Fenster für Optionen des lokalen Filters im Bereich **Allgemeine Optionen** den Namen und das Verhalten des Filters (Traffic erlauben) fest.
4. Geben Sie im Bereich **Quellen** mit Hilfe der Schaltfläche **Hinzufügen** einen IP-Adressenbereich an, aus welchem IP-Adressen für mobile Clients bei ihrer Anbindung an den Coordinator vergeben werden. Dieser Adressenbereich wird beim Einstellen des IPsec-Gatewayprofils definiert (s. Konfiguration des IPsec-Profils für den Windows-Coordinator auf S. 195).

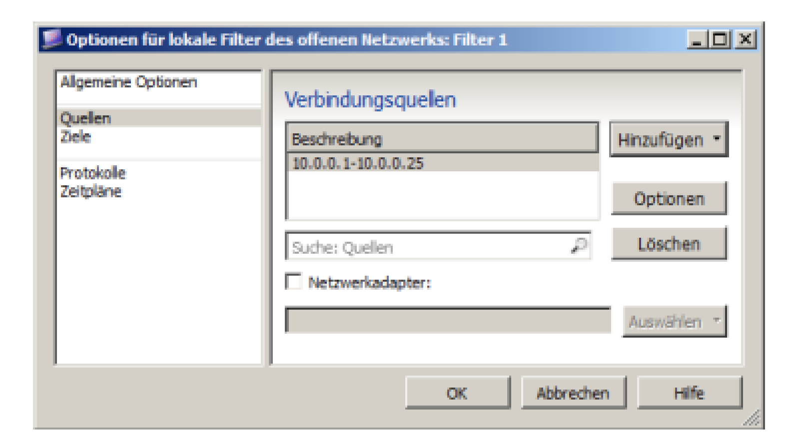


Abbildung 112. IP-Adressen der Smartphone-Clients angeben

5. Klicken Sie im Bereich **Ziele** auf **Hinzufügen** und wählen im Menü den Befehl **Mein ViPNet Knoten**.
6. Führen Sie im Bereich **Protokolle** folgende Aktionen durch:
   - Klicken Sie auf **Hinzufügen** und wählen **TCP/UDP-Protokoll** aus.
   - Wählen Sie im Fenster **TCP/UDP-Protokoll** aus:
     - **Protokoll**: **TCP**.
     - **Quellport**: **Alle Ports**.
     - **Zielport**: **Portnummer**, wählen Sie den Wert `80-http` aus.
     - Klicken Sie auf **OK**.

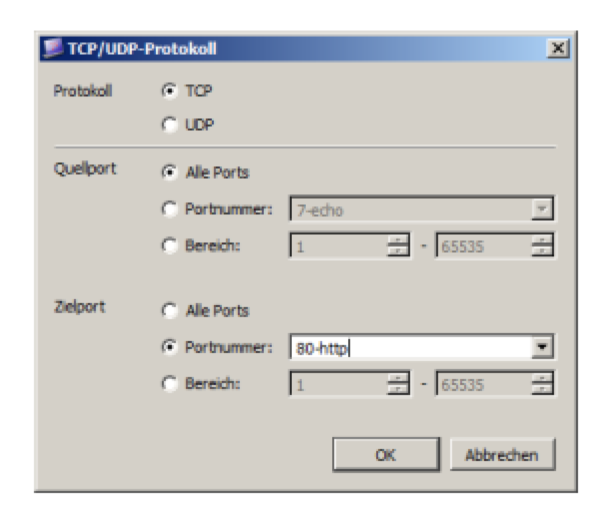


Abbildung 113. Filterparameter für den Zugang zum Web-Server

7 Klicken Sie im Fenster für Optionen des lokalen Filters auf **OK**.

8 Klicken Sie im Bereich **Lokale Filter des offenen Netzwerks** auf **Alle übernehmen**.

Konfiguration von Filter und NAT-Regel für den Zugang von Smartphone-Clients zum Internet

Führen Sie auf dem Coordinator die folgenden Aktionen aus, um Verbindungen mobiler Geräte zu externen Knoten im Internet zu erlauben und um ein korrektes Routing der IP-Pakete sicherzustellen:

- Erstellen Sie im Bereich **Netzwerkfilter** > **Transitregel des offenen Netzwerk** einen Filter für den Transit-Traffic.

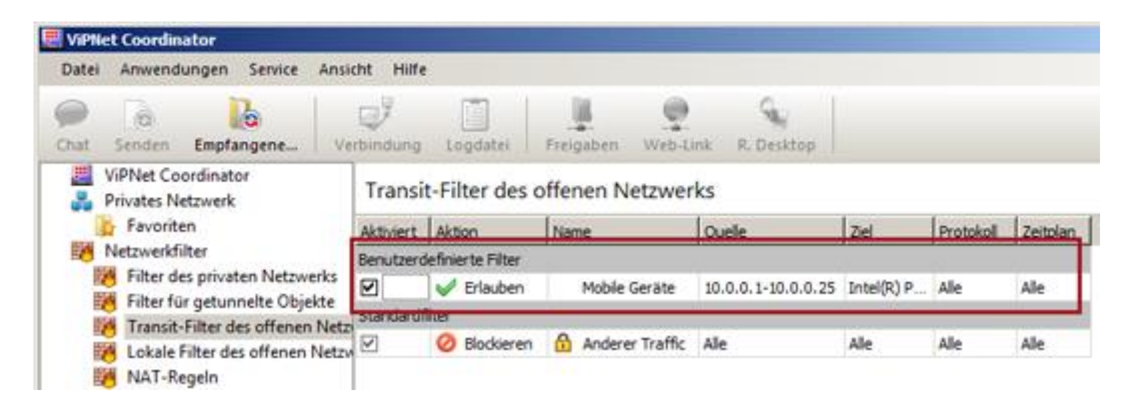


Abbildung 114. Filter für den Transit-Traffic

Geben Sie beim Erstellen des Filters im Fenster für Optionen des Filters im Bereich **Quellen** einen IP-Adressenbereich an, aus dem IP-Adressen für mobile Endgeräte bei ihren Verbindungen zum Coordinator vergeben werden. Dieser Bereich wird bei der Konfiguration des IPsec-Gatewayprofils definiert (s. Konfiguration des IPsec-Profils für den Windows-Coordinator auf S. 195).

Aktivieren Sie im Bereich **Ziele** das Kontrollkästchen **Netzwerkadapter für eingehende Verbindungen** und definieren ein Netzwerkadapter des Coordinators, der an das Internet angeschlossen ist.

Wenn erforderlich, geben Sie im Bereich **Protokolle** die Protokolle und Ports an, über welche die Verbindungen zu Knoten im Internet erlaubt sein sollen.

- Erstellen Sie im Bereich **Netzwerkfilter** > **NAT-Regeln** eine Quellübersetzungsregel.

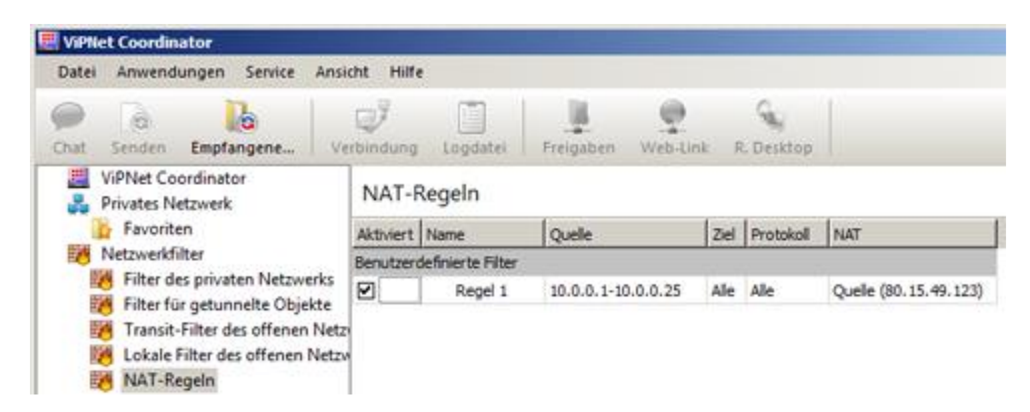


Abbildung 115. Quellübersetzungsregel

Geben Sie beim Erstellen der Regel im Fenster für Regeloptionen im Bereich **Quellen** den Bereich von IP-Adressen an, aus dem Adressen für mobile Endgeräte bei ihrem Verbindungsaufbau zum Coordinator vergeben werden. Aktivieren Sie im Bereich **NAT-Regeln** das Kontrollkästchen **Quelladresse ersetzen durch** und dann wählen **IP-Adresse des ausgehenden Netzwerkadapter (wird automatisch festgelegt)**.

Verwendung eines ViPNet Coordinator HW/VA als IPsec-Gateway für Anbindung mobiler Endgeräte

Wenn in Ihrem Netzwerk ein ViPNet Coordinator HW/VA verwendet wird, dann konfigurieren Sie die IPsec-Gatewayparameter für diesen Coordinator. Im Unterschied zum Windows-Coordinator wird für den ViPNet Coordinator HW/VA nur eine begrenzte Anzahl an Einstellungen benötigt.

Vorgehensweise bei Anbindung von Smartphone-Clients an das ViPNet Netzwerk

Führen Sie die in der unteren Tabelle aufgeführten Schritte aus, um einen neuen IPsec-Gateway einzurichten und um Smartphone-Clients an diesen Server anzubinden.

Tabelle 12. Neuen IPsec-Gateway und Smartphone-Clients hinzufügen

	Aktion	Verweis
☐	Wählen oder erstellen Sie im Programm ViPNet Network Manager einen Coordinator, der die Rolle des IPsec-Gateways übernehmen soll, und konfigurieren die Verbindungsparameter über das IPsec-Protokoll.	Konfiguration von IPsec-Verbindungen für den ViPNet Coordinator HW/VA-Coordinator (auf S. 209)
☐	Wenn der Zugang mobiler Geräte zu geschützten ViPNet Knoten bereitgestellt werden soll, dann definieren bei der Konfiguration des IPsec-Gateways einen Bereich getunnelter IP-Adressen für die Smartphone-Clients.	Konfiguration von IPsec-Verbindungen für den ViPNet Coordinator HW/VA-Coordinator (auf S. 209) Tunnelung (auf S. 114)
☐	Fügen Sie auf dem Coordinator die benötigte Anzahl an Smartphone-Clients hinzu und konfigurieren ihre Parameter.	Profile IPsec für Smartphone-Clients einstellen (auf S. 211)
☐	Konfigurieren Sie die IPsec-Verbindungsparameter.	Konfiguration von IPsec-Verbindungen für den ViPNet Coordinator HW/VA-Coordinator (auf S. 209)

	Aktion	Verweis
☐	Senden Sie die Schlüssel an den ViPNet Coordinator HW/VA. Wenn auf dem Coordinator keine Schlüssel installiert sind, dann erstellen Sie zunächst die Schlüssel für den Coordinator und leiten diese zusammen mit der Konfigurationsdatei `hwinit_set.xml` an den Administrator des Coordinators weiter.	Versenden der Schlüssel-Updates (auf S. 145) Speichern der Schlüsseldistributionen (auf S. 142)
☐	Installieren Sie die IPsec-Profile auf den mobilen Apple-Geräten.	Konfiguration mobiler Geräte von Apple (auf S. 213)
☐	Benutzen Sie die mobilen Endgeräte für den Zugriff auf geschützte ViPNet Netzwerkobjekte.	Konfiguration mobiler Geräte von Apple (auf S. 213)

Führen Sie die nachfolgend aufgezählten Aktionen aus, um Smartphone-Clients für die Anbindung an einen bestehenden IPsec-Coordinator hinzuzufügen.

Tabelle 13. Mobile Clients auf einem bestehenden IPsec-Gateway hinzufügen

	Aktion	Verweis
☐	Fügen Sie auf dem bestehenden IPsec-Coordinator die benötigte Anzahl an mobilen Clients hinzu und konfigurieren ihre Parameter.	Profile IPsec für Smartphone-Clients einstellen (auf S. 211)
☐	Konfigurieren Sie die IPsec-Verbindungsparameter.	Konfiguration von IPsec-Verbindungen für den ViPNet Coordinator HW/VA-Coordinator (auf S. 209)
☐	Senden Sie die Schlüssel an den ViPNet Coordinator HW/VA. Wenn auf dem Coordinator keine Schlüssel installiert sind, dann erstellen Sie zunächst die Schlüssel für den Coordinator und leiten diese zusammen mit der Konfigurationsdatei `hwinit_set.xml` an den Administrator des Coordinators weiter.	Versenden der Schlüssel-Updates (auf S. 145) Speichern der Schlüsseldistributionen (auf S. 142)
☐	Installieren Sie die IPsec-Profile auf den neuen mobilen Apple-Geräten.	Konfiguration mobiler Geräte von Apple (auf S. 213)
☐	Benutzen Sie die neu hinzugefügten mobilen Endgeräte für den Zugriff auf geschützte ViPNet Netzwerkobjekte.	Konfiguration mobiler Geräte von Apple (auf S. 213)

Konfiguration von IPsec-Verbindungen für den ViPNet Coordinator HW/VA-Coordinator

Als IPsec-Gateway kann ein Coordinator verwendet werden, auf welchem die Software ViPNet Coordinator HW/VA installiert ist.

Führen Sie die folgenden Schritte aus, um IPsec-Verbindungen für den ViPNet Coordinator HW/VA einzustellen:

1 Wählen Sie im Programm ViPNet Network Manager in der Navigationsleiste den ViPNet Coordinator HW/VA aus, der als IPsec-Gateway auftreten soll.

2 Öffnen Sie die Registerkarte **IPsec-Verbindung**.

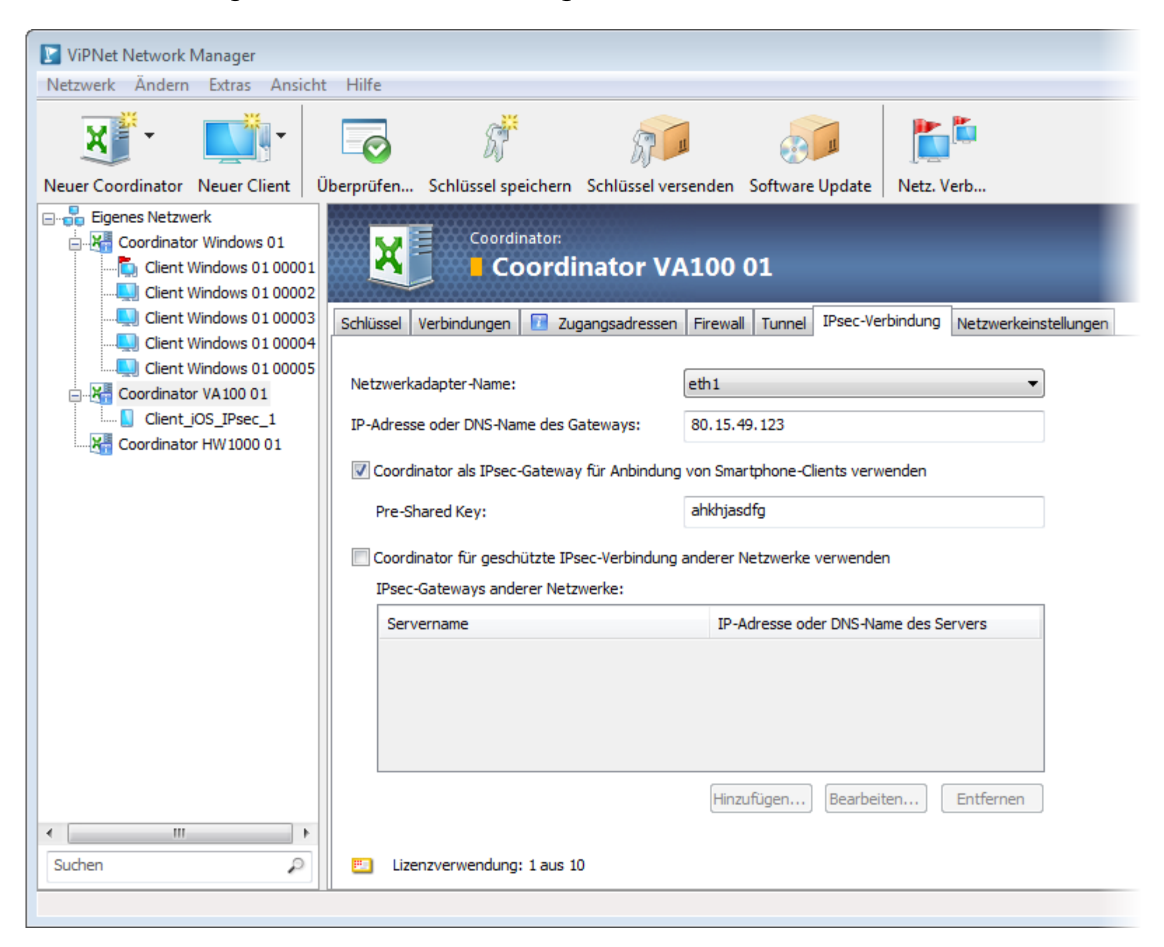


Abbildung 116. Konfiguration der IPsec-Verbindungsparameter für den ViPNet Coordinator HW/VA-Coordinator

3 Damit auf dem Coordinator Smartphone-Clients hinzugefügt werden können, aktivieren Sie das Kontrollkästchen **Coordinator als IPsec-Gateway für Anbindung von Smartphone-Clients verwenden**.



Achtung! Wenn der Coordinator für den Einsatz als IPsec-Gateway bereits konfiguriert ist, werden beim Deaktivieren dieses Kontrollkästchens alle IPsec-Parameter und alle neu hinzugefügten mobilen Clients wieder gelöscht.

4 Wählen Sie in der Liste **Netzwerkadapter-Name** den Netzwerkadapter auf dem Coordinator aus, der für die Verbindungen der Smartphone-Clients verwendet werden soll.

5 Geben Sie im Feld **IP-Adresse oder DNS-Name des Gateways** die öffentliche IP-Adresse oder den DNS-Namen ein, über welche eine Verbindung zum Coordinator aus dem Internet hergestellt werden kann.

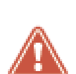


Hinweis. Wenn der Coordinator über keine statische IP-Adresse verfügt, kann für ihn ein DNS-Name mit Hilfe des dynamischen DNS-Dienstes registriert werden.

6 Geben Sie im Feld **Pre-Shared Key** eine beliebige Reihenfolge an Zeichen ein (nicht mehr als 256). Diese Zeichenfolge wird für die Überprüfung der Verbindungsauthentizität verwendet.

7 Wenn der Zugriff von Smartphone-Clients auf geschützte ViPNet Clients sichergestellt werden soll, konfigurieren Sie zunächst eine Tunnelung dieser Geräte durch den Coordinator. Geben Sie dazu in der Registerkarte **Tunnel** des entsprechenden Coordinators (s. Tunnelung auf S. 114) den IP-Adressenbereich für die Smartphone-Clients sowie die maximal zulässige Anzahl an gleichzeitig getunnelten Verbindungen an. Weil mobile Geräte IP-Adresse aus dem Bereich 192.168.30.0/24 bekommen, geben Sie in der Registerkarte **Tunnel** diesen Bereich ein.

IP-Adressen, die in der Registerkarte **Tunnel** angegeben sind, werden als Teil des Schlüsselupdates an den ViPNet Coordinator HW/VA weitergeleitet. Beim Aufbau einer Verbindung zum Coordinator erhält der Smartphone-Client eine IP-Adresse aus dem angegebenen Bereich. Zusätzlich werden diese Adressen als getunnelte Adressen auf dem Coordinator geführt.



Achtung! Die Anzahl getunnelter IP-Adressen des Coordinators muss die Anzahl der Smartphone-Clients, die sich voraussichtlich zu diesem Coordinator verbinden werden, mindestens um eins übersteigen.

Die Anzahl der gleichzeitig getunnelten IP-Adressen sollte die von der Lizenz für ViPNet Coordinator HW/VA erlaubte Anzahl nicht übersteigen.

8 Fügen Sie auf dem Coordinator die benötigte Anzahl an Smartphone-Clients hinzu und konfigurieren ihre Parameter (s. Profile IPsec für Smartphone-Clients einstellen auf S. 211).

9 Klicken Sie in der Panel-Ansicht in der Registerkarte **Schlüssel** auf die Schaltfläche **Schlüssel senden**, um die IPsec-Verbindungseinstellungen an den ViPNet Coordinator HW/VA zu übermitteln.

Wenn auf dem ViPNet Coordinator HW/VA keine Schlüssel installiert sind, klicken Sie auf **Schlüssel speichern** (s. Speichern der Schlüsseldistributionen auf S. 142), um die Schlüssel zu erstellen. Übergeben Sie anschließend die Schlüssel zusammen mit der Konfigurationsdatei `hwinit_set.xml` dem Administrator des Coordinators.

Nachdem die vorgenommenen Einstellungen auf dem ViPNet Coordinator HW/VA angewendet wurden, können Daten mit den Smartphone-Clients über IPsec ausgetauscht werden.

Konfiguration mobiler Geräte

Damit sich ein mobiles Gerät über einen geschützten IPsec-Kanal zum ViPNet Netzwerk verbinden kann, sollten im Programm ViPNet Network Manager ein Smartphone-Client erstellt und ein Benutzername und ein Passwort für den Schutz der Verbindung definiert werden.

Wenn sich ein mobiles Gerät mit dem Betriebssystem iOS zum ViPNet Netzwerk verbinden soll, kann dazu im Programm ViPNet Network Manager ein IPsec-Profil für dieses Gerät erstellt werden. Mit Hilfe dieses Profils können Sie die IPsec-Verbindungsparameter auf dem Gerät automatisch konfigurieren (s. Konfiguration mobiler Geräte von Apple auf S. 213).

Wenn Sie mobile Geräte mit anderen Betriebssystemen (zum Beispiel Android) verwenden, dann sollten Sie die im Programm ViPNet Network Manager definierten IPsec-Verbindungsparameter auf diesen Geräten manuell einstellen.

Profile IPsec für Smartphone-Clients einstellen

Führen Sie die folgenden Schritte aus, um das IPsec-Profil für die Anbindung mobiler Geräte an das ViPNet Netzwerk einzustellen:

1 Fügen Sie auf dem Coordinator, der als IPsec-Gateway verwendet wird, den mobilen Client hinzu (s. Netzwerkknoten hinzufügen auf S. 132).

2 Wählen Sie in der Navigationsleiste den neu angelegten Smartphone-Client aus. Die Parameter des Clients werden in der Panel-Ansicht aufgelistet.

3 Gehen Sie wie folgt vor, um ein Benutzerpasswort anzulegen, das für die Verbindung zum IPsec-Gateway verwendet wird:

   3.1 Klicken Sie auf die Schaltfläche **Passwort ändern**. Es wird das Fenster **Benutzerpasswort** geöffnet.

   3.2 Stellen Sie sicher, dass in der Liste **Passworttyp** der Eintrag **Benutzerdefiniertes** ausgewählt ist.

   3.3 Geben Sie in den entsprechenden Feldern das Passwort und die Passwortbestätigung ein:

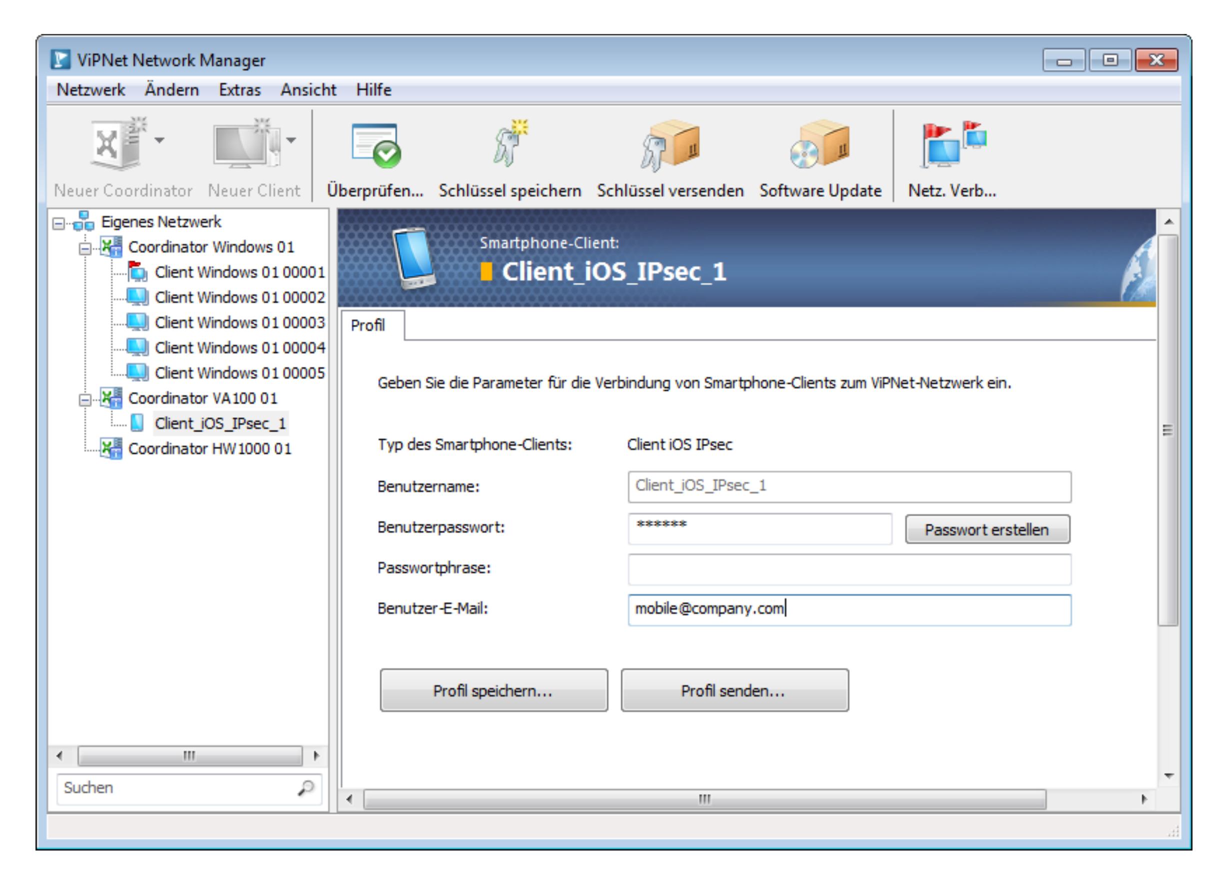


Abbildung 117. Parameter des Smartphone-Clients



Achtung! Das neu angelegte Kennwort muss den auf dem IPsec-Gateway gültigen Passwortrichtlinien entsprechen. Es wird empfohlen, ein Kennwort zu erzeugen, dessen Länge mindestens 6 Zeichen beträgt, und das gleichzeitig Symbole der drei unten aufgelisteten Arten enthält:

- lateinische Großbuchstaben (A-Z).
- lateinische Kleinbuchstaben (a-z).
- Ziffern (0-9).
- Sonderzeichen (zum Beispiel #, %, !, $).

3.4 Klicken Sie auf **OK**.

4 Geben Sie im Feld **Benutzer-E-Mail** eine E-Mail-Adresse zum Versenden des IPsec-Profils an das mobile Gerät ein.

5 Klicken Sie zum Senden der Profildatei an das mobile Endgerät auf die Schaltfläche **Profil versenden**.

Es wird das Standard-E-Mail-Programm gestartet. In diesem Programm wird automatisch eine neue E-Mail-Nachricht erzeugt, die an den Benutzer des Smartphone-Clients gerichtet ist, und das IPsec-Profil als Anlage enthält.

6 Versenden Sie die neue Nachricht.



Hinweis. Wenn das IPsec-Profil aus irgendwelchen Gründen nicht über E-Mail versendet werden kann, speichern Sie die Profildatei mit Hilfe der Schaltfläche **Profil speichern** ab und übertragen die Datei auf das mobile Gerät auf eine andere Art und Weise.

7 Installieren Sie das neu angelegte IPsec-Profil auf dem Apple-Gerät (s. Konfiguration mobiler Geräte von Apple auf S. 213).

Konfiguration mobiler Geräte von Apple

Führen Sie die folgenden Schritte aus, um das IPsec-Profil auf dem mobilen Endgerät Apple iPad oder iPhone zu installieren:

1 Versenden Sie im Programm ViPNet Network Manager das Profil des Smartphone-Clients über E-Mail (s. Profile IPsec für Smartphone-Clients einstellen auf S. 211).

2 Öffnen Sie auf dem Gerät iPad oder iPhone die Nachricht, die das versendete IPsec-Profil als Anhang enthält (Datei mit Erweiterung `.mobileconfig`).



Abbildung 118. Profildatei als Anhang

3 Wählen Sie die angehängte Datei aus. Es wird das Fenster zur Installation des Profils geöffnet.



Abbildung 119. IPSec-Profile installieren

4 Klicken Sie auf **Installieren**. Beim Einblenden einer Warnung, dass das Profil nicht signiert ist, klicken Sie erneut auf **Installieren**.

5 Geben Sie im Passwort-Fenster das Benutzerkennwort ein, das für diesen Smartphone-Client in ViPNet Network Manager angelegt wurde. Dieses Passwort können Sie beim Administrator des ViPNet Netzwerks anfordern.

6 Nach Eingabe des Passworts ist die Installation des Profils abgeschlossen. Klicken Sie auf **Fertig**.

7 Öffnen Sie das Programm **Einstellungen** und wählen in der Navigationsleiste den Bereich **VPN**, um die Parameter des installierten Profils zu konfigurieren.



Abbildung 120. VPN-Konfigurationen

8 Wählen Sie in der Panel-Ansicht das installierte IPsec-Profil.

9 Klicken Sie im Fenster mit den Profileigenschaften im Bereich **Proxy** auf **Aus**.



Abbildung 121. Proxy deaktivieren

10 Klicken Sie auf **Sichern**.

Die Installation und die Konfiguration des Profils sind nun abgeschlossen.

Zum Aufbau einer Verbindung zum ViPNet Netzwerk öffnen Sie das Programm **Einstellungen** und wählen **Allgemeine** > **Netzwerk** > **VPN**, dann setzen Sie den Schalter auf .

Wenn Sie auf Objekte im geschützten Netzwerk zugreifen möchten, geben Sie in der Adresszeile des Browsers oder einer anderen Anwendung die IP-Adresse oder den DNS-Namen des geschützten ViPNet Knotens ein.

9

Arbeit mit dem Programm ViPNet Client für Windows

Installation der Schlüsseldistribution

Für den ordnungsgemäßen Betrieb der Software ViPNet Client und ViPNet Coordinator sollten ViPNet Schlüssel auf den Netzwerkknoten installiert werden. Die Datei *.dst, die eine Schlüsseldistribution enthält, können Sie beim ViPNet Netzwerkadministrator anfordern.

Führen Sie zum Installieren der Schlüssel die folgenden Aktionen aus:

1. Doppelklicken Sie auf die Schlüsseldistribution (Datei *.dst), die für Ihren Netzwerkknoten bestimmt ist. Es wird der Assistent **ViPNet Schlüsselinstallation** gestartet.
2. Stellen Sie sicher, dass eine Schlüsseldistribution ausgewählt ist, die für Ihren Netzwerkknoten bestimmt ist. Der Name des Netzwerkknotens und der Benutzername werden unterhalb des Felds mit dem Dateipfad zur Schlüsseldistribution angezeigt. Klicken Sie, wenn nötig, auf **Durchsuchen**, um den Standort der Schlüsseldistribution anzugeben.

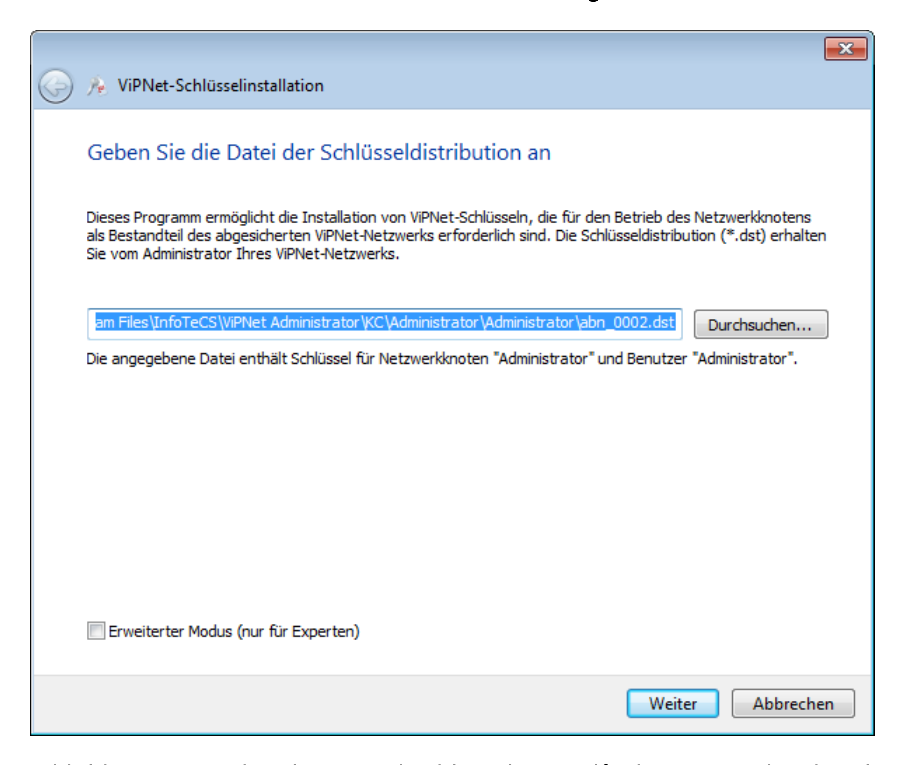


*Abbildung 122. Adresslisten und Schlüssel mit Hilfe der Datei *.dst aktualisieren*

3. Klicken Sie auf die Schaltfläche **Schlüssel installieren**, um die Installation zu starten.
4. Nachdem die Schlüssel erfolgreich installiert wurden, wird eine entsprechende Meldung angezeigt. Klicken Sie auf die Schaltfläche **Schließen**, um den Assistenten zu beenden.
5. Nach der erfolgreichen Installation der Schlüssel kann nun das Programm ViPNet Client oder ViPNet Coordinator gestartet werden.

Start des Programms ViPNet Monitor

Standardmäßig wird das Programm ViPNet Monitor sofort nach der Authentifizierung des ViPNet Benutzers, die beim Starten des Betriebssystems Windows durchgeführt wird, automatisch gestartet.



Achtung! Die Initialisierung des ViPNet Treibers wird am Beginn des Startvorgangs von Windows durchgeführt, d. h. noch vor der Initialisierung anderer Dienste und Treiber des Betriebssystems. Die Arbeit des ViPNet Treibers vor der Authentifizierung des ViPNet Benutzers wird standardmäßig von vorinstallierten Filtern des privaten Netzwerks sowie zusätzlich von den Filtern des offenen Netzwerks, die in der letzten Sitzung verwendet wurden, geregelt.

Wenn Sie das Programm beendet haben oder die Authentifizierung abgelehnt haben, dann führen Sie folgende Schritte durch, um ViPNet Monitor zu starten:

1 Führen Sie einen der folgenden Schritte aus:

- Verwenden Sie das Betriebssystem Windows 7, Windows Server 2008 R2 oder eine frühere Version, wählen Sie im Menü **Start** den Eintrag **Alle Programme** > **ViPNet** > **ViPNet Client** (oder **Coordinator**) > **Monitor**.
- Verwenden Sie das Betriebssystem Windows 8, Windows Server 2012 oder eine spätere Version, öffnen Sie die Apps-Liste auf der Startseite und wählen den Eintrag **ViPNet** > **Monitor**.

Das Anmeldefenster des Programms wird geöffnet.

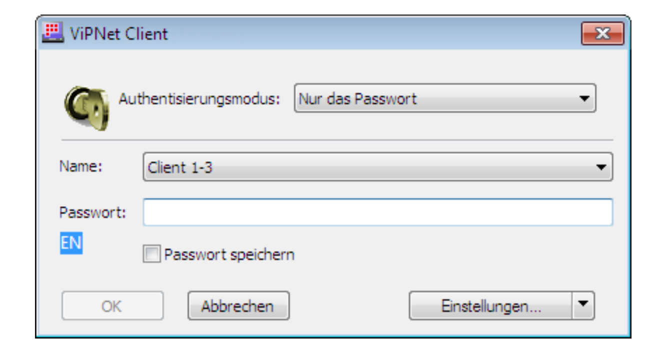


Abbildung 123. Anmeldefenster des Programms

Wählen Sie den passenden Authentisierungsmodus (s. Authentisierungsmodi auf S. 335) für die Anmeldung, dann in Abhängigkeit vom gewählten Authentisierungsmodus geben entweder das Benutzerpasswort ein oder schließen ein externes Authentisierungsgerät an und geben dann eine PIN ein.

2 Nachdem alle für die Autorisierung erforderliche Eingaben gemacht wurden, klicken Sie auf **OK**. Das Hauptfenster von ViPNet Monitor wird geöffnet.

Benutzerinterface von ViPNet Client Monitor

Das Fenster des Programms ViPNet Client Monitor ist in der folgenden Abbildung dargestellt:

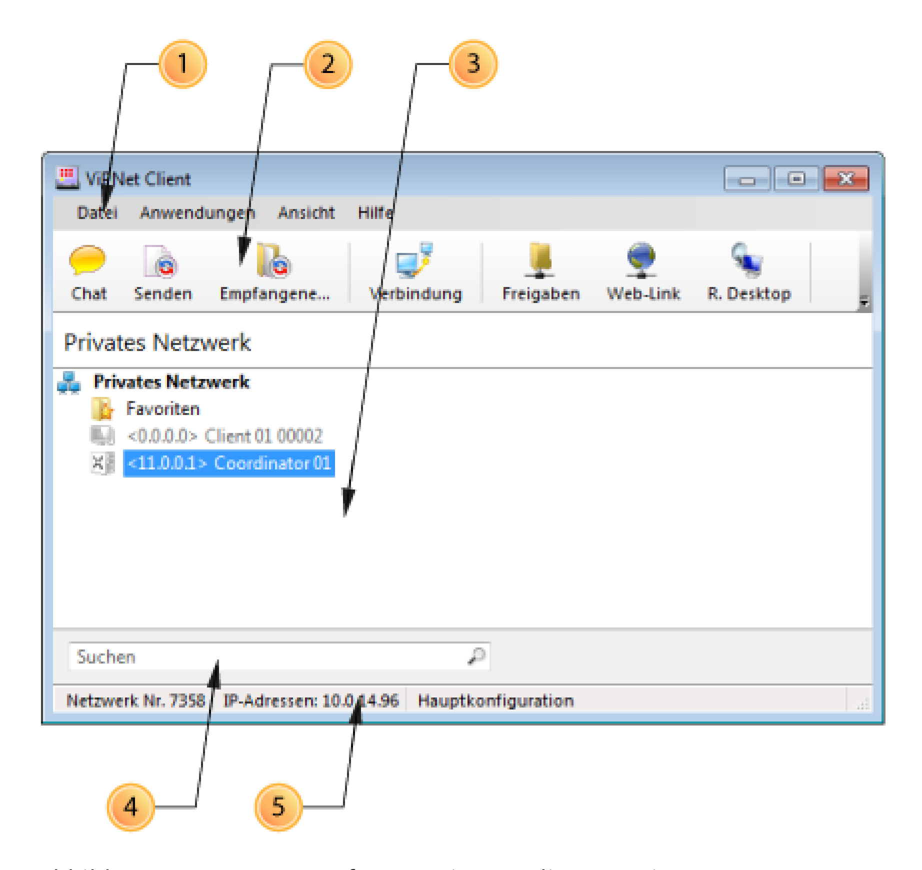


Abbildung 124. Programmfenster ViPNet Client Monitor

Mit den Zahlen sind gekennzeichnet:

1. Das Hauptmenü des Programms.
2. Die Symbolleiste. Um Symbole anzeigen oder verstecken, wählen Sie die Option **Symbolleiste** im Menü **Ansicht** aus. Ebenso können Sie die Schaltflächen in der Symbolleiste mit Hilfe der Schaltfläche . Ziehen Sie zum Ändern der Schaltflächenpositionen in der Symbolleiste die betroffene Schaltfläche auf die gewünschte Stelle, während Sie die **ALT**-Taste gedrückt halten.

   Wenn auf einem Client das Programm ViPNet Business Mail zugewiesen ist, erschient auf der Symbolleiste auch die Schaltfläche **B-Mail** .
3. Panel-Ansicht. Enthält die Liste der ViPNet Netzwerkknoten, die mit dem gegebenen Netzwerkknoten im Programm ViPNet Network Manager verbunden sind.
4. Das Suchfeld. Für eine Suche eines Netzwerkknotens tragen Sie im Suchfeld einen Teil der Adresse oder des Namens sowie ggf. andere Parameter ein.

- Netzwerkknotenname (wird im Panel-Ansicht und im Fenster **Netzwerkknoten-Eigenschaften** in der Registerkarte **Allgemeine** angezeigt).
- Computername (das Fenster **Netzwerkknoten-Eigenschaften**, die Registerkarte **Allgemeine**).
- Alias (das Fenster **Netzwerkknoten-Eigenschaften**, die Registerkarte **Allgemeine**).
- Reelle und virtuelle IP-Adresse (das Fenster **Netzwerkknoten-Eigenschaften**, die Registerkarte **IP-Adressen**, die Liste **IP-Adressen**).
- DNS-Name (das Fenster **Netzwerkknoten-Eigenschaften**, die Registerkarte **IP-Adresse**, die Liste **DNS-Name**).
- Netzwerkknoten-ID (das Fenster **Netzwerkknoten-Eigenschaften**, die Registerkarte **Allgemeine**).

5 Die Statusleiste. Enthält die folgenden Informationen: Nummer des ViPNet Netzwerks, dem Knoten zugewiesene IP-Adressen, laufende Konfiguration des Programms. Bei Änderungen der Netzwerkfilter oder Objektgruppen wird statt der angegebenen Daten eine Meldung in der Statusleiste eingeblendet, dass die Filter oder Objektgruppen geändert, jedoch noch nicht übernommen wurden.

Damit die Statusleiste ein- oder ausgeblendet wird, wählen Sie im Menü **Ansicht** den Eintrag **Statusleiste**. Beim Vorliegen von Änderungen in den Filtern oder Objektgruppen wird die Statusleiste immer angezeigt, auch wenn sie zuvor ausgeblendet wurde.

Auf den Clients des Netzwerks ViPNet VPN wird eine Programmversion von ViPNet Monitor verwendet, die eine vereinfachte Oberfläche besitzt. Den Benutzern stehen dabei die folgenden Programmfunktionen zur Verfügung:

- Arbeiten mit der Liste der geschützten Knoten (s. Arbeiten mit der ViPNet Netzwerkknotenliste auf S. 220);
- FileExchange (s. Empfang von Dateien auf S. 223);
- Austausch von Nachrichten (Chat) (s. Verschlüsselter Chat auf S. 222);
- Anzeige der Webressourcen und der freigegebenen Objekte auf den Netzwerkknoten;
- Annahme von Updates für Schlüssel, Software und Sicherheitsrichtlinien (s. Empfang von Updates auf S. 224);
- Arbeiten mit den Programmen ViPNet SafeDisk-V und ViPNet Business Mail, falls die Verwendung dieser Programme vom Netzwerkadministrator erlaubt wurde.

Das Passwort kann über das Menü **Datei** > **Benutzerpasswort ändern** geändert werden. Bei dieser Vorgehensweise kann der Typ des Passworts nicht geändert werden. Außerdem kann das Benutzerpasswort von ViPNet Client Monitor im Administratormodus geändert werden (s. Benutzerpasswort ändern auf S. 333).

Nach der Anmeldung im Programm ViPNet Client Monitor im Administratormodus wird die vollständige Benutzeroberfläche angezeigt. Es stehen erweiterte Programmeinstellungen zur Verfügung.

Die Konfiguration des Programms ViPNet Monitor, der Netzwerkfilter und des Zugangs zu den anderen Knoten kann auf dem Client im Administratormodus durchgeführt werden (s. Arbeiten mit Administratorrechten auf S. 338).

Arbeiten mit der ViPNet Netzwerkknotenliste

Der Bereich **Privates Netzwerk** enthält eine Liste aller ViPNet Netzwerkknoten, die mit dem eigenen Netzwerkknoten verbunden sind. Diese Verbindungen werden in ViPNet Network Manager definiert.

Das Symbol neben dem Namen eines Netzwerkknotens sowie seine Farbe kennzeichnen den Typ und Status des Netzwerkknotens:

Tabelle 14. Kennzeichnung des Netzwerkknotenstatus

Symbol	Namefarbe	Status
	Grau	Client ist z.Zt. nicht mit dem Netzwerk verbunden oder es gibt keine Angaben zu seinem Status
	Violett	Client ist mit dem Netzwerk verbunden
	Grau oder violett, halbfett dargestellt	Neuer Client, zu dem eine Verbindung erstellt wurden
	Grau oder violett, halbfett dargestellt	Neuer Coordinator, zu dem eine Verbindung erstellt wurde
	Grau	Coordinator ist z.Zt. nicht mit dem Netzwerk verbunden oder es gibt keine Angaben zu seinem Status
	Violett	Coordinator ist mit dem Netzwerk verbunden

Netzwerkknoten im Bereich **Privates Netzwerk** können aus praktischen Gründen in Ordnern gruppiert werden:

- Zum Erstellen eines neuen Ordners, klicken Sie im Programmfenster von ViPNet Monitor in der Navigationsleiste oder auf der Panel-Ansicht mit der rechten Maustaste auf den Eintrag **Privates Netzwerk** und wählen im Kontextmenü den Punkt **Ordner erstellen**.

  Der neue Ordner wird in der Navigationsleiste und im Bereich **Privates Netzwerk** angezeigt.

- Wenn Sie bestimmte Netzwerkknoten in irgendeinen Ordner verschieben möchten, wählen Sie im Bereich **Privates Netzwerk** einen oder mehrere Knoten aus und ziehen diese in den benötigten Ordner.
- Wenn Sie einen Ordner umbenennen möchten, klicken Sie mit der rechten Maustaste auf diesen Ordner und wählen im Kontextmenü **Umbenennen**.
- Zum Löschen der Ordner:

- Stellen Sie sicher, dass die zu löschenden Ordner keine Netzwerkknoten enthalten. Ansonsten verschieben Sie die Netzwerkknoten in andere Ordner.
- Wählen Sie einen oder mehrere Ordner im Navigationsbereich oder im Bereich **Privates Netzwerk** aus.
- Drücken Sie die **Entf**-Taste oder wählen im Kontextmenü den Befehl **Löschen**.

Geben Sie einen Teil des Namens, eine IP-Adresse oder andere Parameter des Knotens in der Suchzeile ein, um einen Netzwerkknoten in der Liste zu suchen.

Doppelklicken Sie auf den Knotennamen, um die Eigenschaften eines Netzwerkknotens anzuzeigen. Es wird das Fenster **Netzwerkknoten-Eigenschaften** geöffnet, in welchem allgemeine Informationen über diesen Netzwerkknoten sowie Einstellungen für den Knotenzugang enthalten sind.

Führen Sie eine der folgenden Aktionen aus, um die Verbindung zu einem anderen Knoten zu prüfen, um eine Sitzung zum Austausch verschlüsselter Nachrichten zu starten, um eine Datei zu versenden oder andere eingebaute Funktionen des Programms ViPNet Monitor zu nutzen:

- Wählen Sie den Knoten in der Liste aus und klicken auf die entsprechende Schaltfläche in der Symbolleiste.
- Wählen Sie den entsprechenden Eintrag im Kontextmenü des Netzwerkknotens.

Verschlüsselter Chat

ViPNet Benutzer können in Echtzeit Sofortnachrichten mit anderen ViPNet Benutzern austauschen oder an einer Konferenz mir mehreren Benutzern teilnehmen:

- Sie können eine Chat-Sitzung starten, um Nachrichten an einen oder mehrere Benutzer gleichzeitig zu senden und die Antworten dieser Benutzer zu empfangen. Die teilnehmenden Benutzer erhalten dabei Ihre Nachrichten, jedoch keine Antwortnachrichten anderer Benutzer.

  Wählen Sie zum Starten einer Chat-Sitzung im Programmfenster von ViPNet Monitor in der Navigationsleiste den Bereich **Privates Netzwerk**. Wählen Sie dann in der rechten Leiste einen oder mehrere Netzwerkknoten aus. Wählen Sie im Kontextmenü für Netzwerkknoten den Befehl **Chat** oder klicken in der Symbolleiste auf die Schaltfläche **Chat** .

- Sie können eine Konferenz unter Beteiligung mehrerer Benutzer starten, damit alle Teilnehmer der Sitzung die Nachrichten aller anderen Benutzer lesen und beantworten können. Darin besteht der Unterschied zwischen einer Konferenz und einer Chat-Sitzung.

  Wählen Sie zum Starten einer Konferenz im Programmfenster von ViPNet Monitor in der Navigationsleiste den Bereich **Privates Netzwerk**. Wählen Sie dann in der rechten Leiste einen oder mehrere Netzwerkknoten aus. Wählen Sie im Kontextmenü für Netzwerkknoten den Befehl **Konferenz einrichten** oder klicken in der Symbolleiste auf die Schaltfläche **Konferenz** (diese Schaltfläche ist standardmäßig ausgeblendet).

Ein ViPNet Benutzer kann gleichzeitig an mehreren Chat-Sitzungen teilnehmen. Beim Empfang einer Nachricht, die zu keiner der aktuellen Sitzungen gehört, wird eine neue Chat-Sitzung geöffnet.

Alle während einer Sitzung gesendeten und empfangenen Nachrichten werden im Sitzungsprotokoll gespeichert. Das Sitzungsprotokoll kann in einer Text-Datei gespeichert werden. Wenn im Rahmen einer Sitzung eine Nachricht an einen Benutzer gesendet wurde, wird seine Antwort im selben Protokoll gespeichert. Das Protokoll der Sitzung kann bei Bedarf als Textdatei gespeichert werden.

Während einer Chat-Sitzung können Sie Dateien und E-Mails an die Teilnehmer versenden.



Hinweis. Wenn die Anwendung Verschlüsselter Chat auf Ihrem Netzwerkknoten nicht verfügbar ist, dann wenden Sie sich an den ViPNet Netzwerkadministrator, damit diese Anwendung freigegeben wird.

Empfang von Dateien

Mit Hilfe der Anwendung „FileExchange“ können sich die Benutzer des ViPNet Netzwerks gegenseitig Dateien über einen geschützten VPN-Kanal senden. Es gibt keine Beschränkungen hinsichtlich des Typs und der Größe der übermittelten Dateien. Zusätzlich wird die Integrität der Dateien überprüft. Wenn die Integrität einer Datei beim Versand verletzt wurde, dann wird die betroffene Datei automatisch gelöscht.



Hinweis. Für Dateien, die von Benutzern gesendet wurden, die mit ViPNet Software einer früheren Version arbeiten, wird die Integritätsüberprüfung nicht durchgeführt. Im Fenster **FileExchange** wird bei solchen Dateien der Status **Integrität nicht verifiziert** angezeigt. Die Entscheidung über die Weiterverwendung einer solchen Datei trifft der Benutzer.

Sie können die Anwendung „FileExchange“ aus dem Programm ViPNet Monitor oder aus dem Kontextmenü von Windows aufrufen.

Wenn Sie eine Datei mit Hilfe des Programms ViPNet Monitor versenden möchten, dann wählen Sie zunächst in der Panel-Ansicht einen oder mehrere Netzwerkknoten aus, an welche die Datei versendet werden soll. Klicken Sie in der Symbolleiste auf die Schaltfläche **Senden** oder wählen im Kontextmenü den Befehl **Datei senden**. Geben Sie im eingeblendeten Fenster die Dateien oder Ordner an, die versendet werden sollen, und klicken dann auf **Öffnen**.

Wenn Dateien von einem anderen ViPNet Benutzer eintreffen, blendet das Programm eine Meldung über die empfangene Datei ein. Im Infobereich der Taskleiste wird das Symbol des FileExchange-Programms angezeigt.

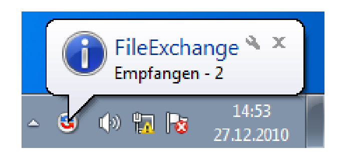


Abbildung 125. Mitteilung über empfangene Dateien

Klicken Sie zum Anzeigen der empfangenen Dateien auf das Programmsymbol von FileExchange im Infobereich der Taskleiste. Es wird das Fenster **FileExchange** geöffnet. Wählen Sie die benötigte Datei in Gruppe **Empfangene Dateien** aus und klicken auf den Namen der Datei in Spalte **Datei**.

Empfang von Updates

Damit die Funktionsfähigkeit des Netzwerkknotens gewährleistet bleibt, kann der ViPNet Netzwerkadministrator mit Hilfe des Programms ViPNet Network Manager Schlüsselupdates (s. Versenden der Schlüssel-Updates auf S. 145) und ViPNet Softwareupdates (s. Versenden von ViPNet Softwareupdates auf S. 149) an den Netzwerkknoten versenden. Die Schlüssel sollten dann aktualisiert werden, wenn der ViPNet Netzwerkadministrator irgendwelche Änderungen an der Struktur des Netzwerks oder an den Einstellungen der einzelnen Netzwerkknoten vornimmt (zum Beispiel neue Verbindungen zwischen den Netzwerkknoten definiert).

Außerdem können vom Administrator des Programms ViPNet Policy Manager (auf S. 37) Sicherheitsrichtlinien an den Netzwerkknoten versendet werden, um die Parameter der integrierten Firewall, die Teil der ViPNet Software ist, zu steuern.

Die Übernahme und Installation der Updates wird auf den Netzwerkknoten mit Hilfe des ViPNet Updatesystems durchgeführt. In Abhängigkeit von den Einstellungen des Updatesystems können die erhaltenen Schlüssel-, Sicherheitsrichtlinien- und Softwareupdates automatisch oder manuell installiert werden.

Die Installation der Updates kann sowohl automatisch (s. Automatische Installation von Updates auf S. 225) als auch manuell (s. Manuelle Installation der Updates auf S. 226) durchgeführt werden.

Wenn auf dem Knoten die manuelle Installation von Updates eingestellt ist, dann wird beim Eintreffen von Updatedateien im Infobereich der Taskleiste das Symbol **ViPNet Updatesystem** mitsamt den entsprechenden Informationen angezeigt.

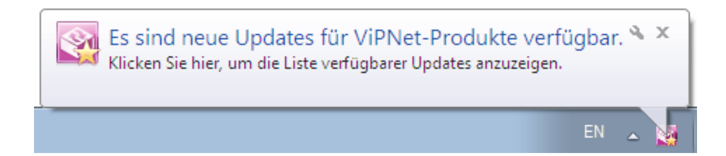


Abbildung 126. Im Infobereich eingeblendete Benachrichtigung über vorhandene Updates

Das Symbol **ViPNet Updatesystem** im Infobereich der Taskleiste kann folgendermaßen aussehen:

- – neue Updates sind verfügbar;
- – Updates wurden erfolgreich installiert;
- – Updates wurden erfolgreich installiert, Neustart erforderlich.

Nach der erfolgten Installation wird das Symbol des Updatesystems nicht mehr im Infobereich angezeigt, falls kein Neustart erforderlich ist.

Wenn auf dem Knoten die automatische Installation von Updates eingestellt ist, dann werden alle Aktionen vom ViPNet Updatesystem im „leisen" Modus ohne Ausgabe von Meldungen auf dem Bildschirm durchgeführt. Im Infobereich der Taskleiste wird das Symbol des Updatesystems nur dann angezeigt, wenn ein Neustart des Computers erforderlich ist (das Symbol wird in Form von angezeigt).

Automatische Installation von Updates



Hinweis. Es wird davon abgeraten, die automatische Annahme von Updates zu aktivieren, falls geschützte SafeDisk-V-Container verwendet werden. Bei Einsatz geschützter SafeDisk-V-Container können die eintreffenden Updates unabhängig vom gewählten Installationsmodus ausschließlich manuell installiert werden.

Wenn Sie möchten, dass die Updates automatisch auf dem Netzwerkknoten installiert werden, führen Sie die folgenden Schritte aus:

1 Melden Sie sich im Betriebssystem mit Administratorrechten an.

  Ohne Administratorrechte können Sie die Einstellungen des ViPNet Updatesystems nicht ändern.

2 Führen Sie einen der folgenden Schritte durch:

  - Verwenden Sie das Betriebssystem Windows 7, Windows Server 2008 R2 oder eine frühere Version, wählen Sie im Menü **Start** den Eintrag **Alle Programme** > **ViPNet** > **ViPNet Updatesystem**.
  - Verwenden Sie das Betriebssystem Windows 8, Windows Server 2012 oder eine spätere Version, öffnen Sie die Apps-Liste auf der Startseite und wählen den Eintrag **ViPNet** > **ViPNet Updatesystem**.

3 Aktivieren Sie im eingeblendeten Fenster in der Registerkarte **Einstellungen** das Kontrollkästchen **Updates automatisch installieren**.

4 Wenn Sie möchten, dass ein Neustart des Computers (falls erforderlich) nach der Installation der Updates automatisch durchgeführt wird, aktivieren Sie das entsprechende Kontrollkästchen.

5 Klicken Sie auf **OK**, um die Einstellungen zu speichern.

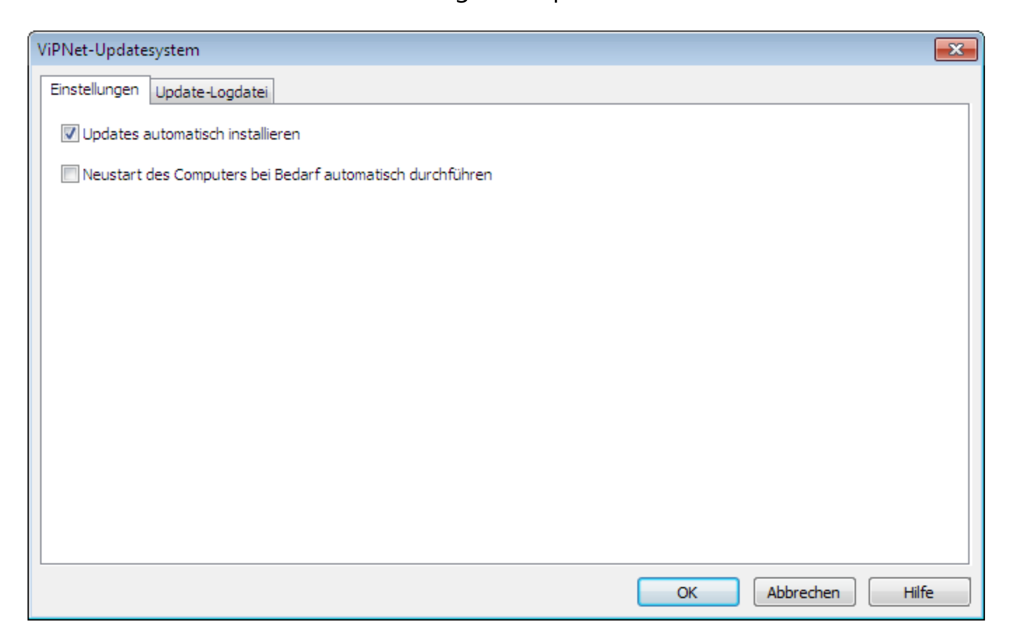


Abbildung 127. Einstellungen des ViPNet Updatesystems

Manuelle Installation der Updates

Wenn Sie die Installation von Updates auf dem Netzwerkknoten selbständig steuern möchten, dann deaktivieren Sie die automatische Update-Installation. Führen Sie dazu die folgenden Schritte aus (s. Abbildung 127 auf S. 225):

1 Melden Sie sich im Betriebssystem mit Administratorrechten an.

   Ohne Administratorrechte können Sie die Einstellungen des ViPNet Updatesystems nicht ändern.

2 Führen Sie einen der folgenden Schritte durch:

   - Verwenden Sie das Betriebssystem Windows 7, Windows Server 2008 R2 oder eine frühere Version, wählen Sie im Menü **Start** den Eintrag **Alle Programme** > **ViPNet** > **ViPNet Updatesystem**.
   - Verwenden Sie das Betriebssystem Windows 8, Windows Server 2012 oder eine spätere Version, öffnen Sie die Apps-Liste auf der Startseite und wählen den Eintrag **ViPNet** > **ViPNet Updatesystem**.

3 Deaktivieren Sie im eingeblendeten Fenster auf der Registerkarte **Einstellungen** das Kontrollkästchen **Updates automatisch installieren**.

4 Wenn Sie möchten, dass ein Neustart des Computers (falls erforderlich) nach der Installation der Updates automatisch durchgeführt wird, aktivieren Sie das entsprechende Kontrollkästchen.

5 Klicken Sie auf **OK**, um die Einstellungen zu speichern.

Wenn die automatische Installation von empfangenen Updates deaktiviert ist, dann installieren Sie die Updates manuell:

1 Klicken Sie im Infobereich der Taskleiste auf das Symbol **ViPNet Updatesystem** mit der rechten Maustaste und wählen im Kontextmenü den Bereich **Verfügbare Updates**.

2 Überprüfen Sie im eingeblendeten Fenster die Liste der zu installierenden Updates (diese sind durch ein Häkchen gekennzeichnet). Wenn ein bestimmtes Update nicht installiert werden soll, deaktivieren Sie das entsprechende Kontrollkästchen.

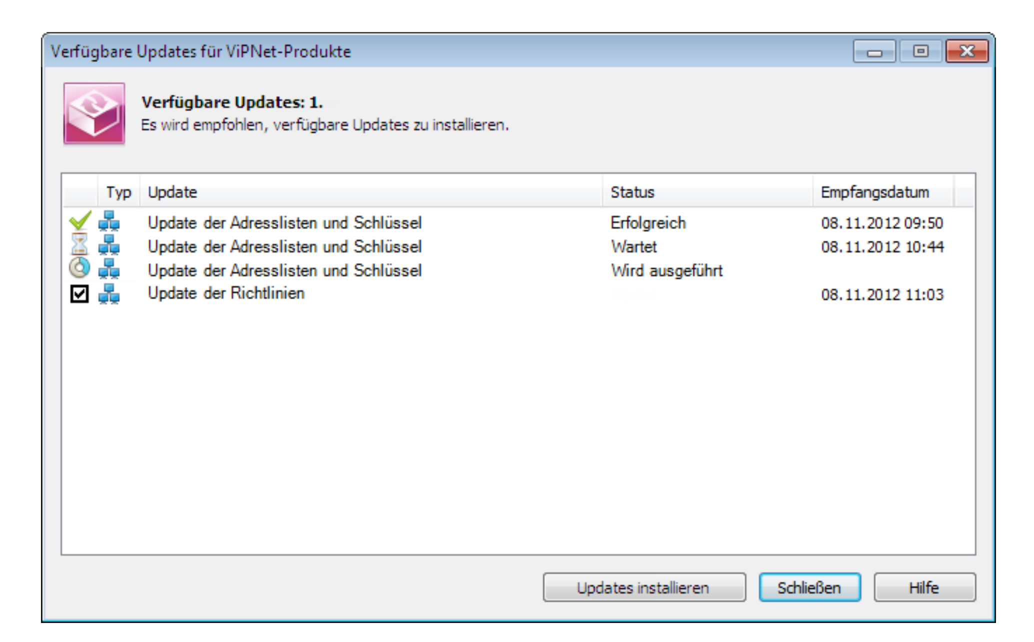


Abbildung 128. Anzeige der erhaltenen Updates

3 Klicken Sie auf die Schaltfläche **Updates installieren**.

4 Falls zum Fortsetzen der Updateinstallation bestimmte ausgeführte Anwendungen beendet werden sollten, wird eine entsprechende Meldung im Fenster **Installation der ViPNet Produktupdates** angezeigt. Klicken Sie auf die Schaltfläche **Fortfahren**. Die betroffenen Anwendungen werden dabei automatisch geschlossen und die Installation der Updates wird fortgesetzt.

Nach dem Starten der Installation wird das Programm ViPNet Monitor aus dem Computerspeicher entladen und der Updatevorgang wird eingeleitet. Diesbezügliche Meldungen werden dabei im Infobereich der Taskleiste angezeigt.

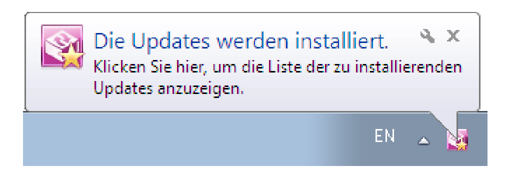


Abbildung 129. Anzeige der Installation von Updates



Achtung! Der Updatevorgang kann eine längere Zeit in Anspruch nehmen. Unterbrechen Sie nicht den Vorgang und starten Sie den Computer nicht neu, bis die Aktualisierung abgeschlossen ist.

5 Wenn nach der Durchführung des Updates ein Neustart erforderlich ist, wird eine entsprechende Meldung im Infobereich der Taskleiste eingeblendet.

Arbeit mit ViPNet Business Mail

Das Programm ViPNet Business Mail wird zum Austausch von elektronischen Nachrichten im geschützten ViPNet Netzwerk verwendet. Benutzer, deren Netzwerkknoten im Programm ViPNet Network Manager miteinander verbunden sind, können Nachrichten mit Hilfe des Programms ViPNet Business Mail untereinander austauschen.

Damit das Programm ViPNet Business Mail auf den Netzwerkclients verwendet werden kann, sollten folgende Bedingungen erfüllt sein:

- Die maximale Anzahl an Clients, auf denen das Programm ViPNet Business Mail installiert werden kann, sollte in der Lizenz von ViPNet VPN (in der entsprechenden Erweiterung) angegeben werden.
- Das Programm ViPNet Business Mail sollte für alle betroffenen Clients im Programm ViPNet Network Manager zur Verwendung freigegeben werden.

Nachdem die Verwendung des Programms erlaubt und das Schlüsselupdate auf dem betroffenen Knoten durchgeführt wurde, kann das Programm ViPNet Business Mail auf den Knoten installiert werden (s. Installation des Programms ViPNet Business Mail auf S. 229).

Beim Update von ViPNet VPN einer früheren Version wird die Möglichkeit zur Verwendung des Programms ViPNet Business Mail für alle Clients zunächst blockiert. Deswegen sollte die Nutzung dieses Programms nach der Aktualisierung der Software für alle betroffenen Clients erlaubt und ein entsprechendes Schlüsselupdate versendet werden. Anschließend kann das Programm ViPNet Business Mail auf den gegebenen Clients wieder ausgeführt werden.



Hinweis. Das vorliegende Kapitel beinhaltet eine kurze Beschreibung des Programms ViPNet Business Mail. Ausführliche Informationen sind in der Programm-Hilfe enthalten (Aufruf durch Drücken der **F1**-Taste oder über das Menü **Hilfe**).

Die Benutzeroberfläche des Programms ist den Oberflächen verbreiteter Mail-Clients (wie Microsoft Outlook) nachempfunden; deswegen ist für die Arbeit mit ViPNet Business Mail keine spezielle Schulung der Benutzer nötig. ViPNet Business Mail bietet die folgenden Funktionen

- Senden und Empfangen von Nachrichten;
- Senden und Empfangen von Nachrichten mit Anhängen;
- Signieren von Nachrichten und Anhängen mit digitaler Signatur;
- Verschlüsseln von Dateien und Anhängen.

Wählen Sie zum Starten von ViPNet Business Mail im Menü **Anwendungen** den Befehl **Business Mail**. Es wird das Programmfenster von ViPNet Client Business Mail geöffnet (s. Benutzeroberfläche von ViPNet Business Mail auf S. 230).

Wenn eine neue Nachricht empfangen wird und ViPNet Business Mail dabei nicht gestartet ist, blendet das MFTP-Modul eine Meldung über den Erhalt der Nachricht ein. Falls im Meldungsfenster das Kontrollkästchen **Business Mail aufrufen** aktiviert ist, wird ViPNet Business Mail nach dem Klicken auf **OK** gestartet.

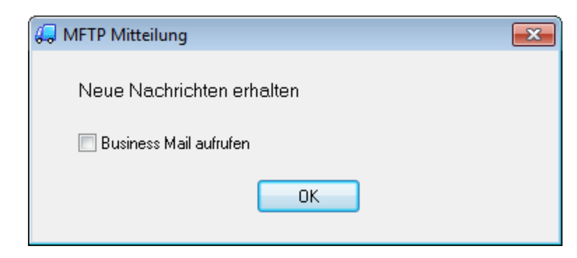


Abbildung 130. Meldung über den Erhalt neuer Nachrichten

Installation des Programms ViPNet Business Mail

Führen Sie die folgenden Schritte aus, um das Programm ViPNet Business Mail auf einen Netzwerkclient zu installieren:

1. Erlauben Sie im Programm ViPNet Network Manager das Programm ViPNet Business Mail auf Clients zu verwenden (s. Verwendung zusätzlicher ViPNet Komponenten auf S. 123).
2. Wählen Sie im Navigationsbereich einen Client und klicken in der Panel-Ansicht in der Registerkarte **Schlüssel** auf die Schaltfläche **Schlüssel versenden**.
3. Beenden Sie auf dem Client nach dem Schlüsselupdate alle offenen Anwendungen und starten das Installationsprogramm von ViPNet VPN.
4. Klicken Sie im Fenster **Installation von ViPNet VPN** auf die Schaltfläche **ViPNet Client aktualisieren...**
5. Wählen Sie im Fenster **Komponenten hinzufügen oder entfernen** die Option **Komponenten hinzufügen oder entfernen**.

   Wenn der Neustart des Computers nach der Fertigstellung der Softwareänderungen automatisch durchgeführt werden soll, dann aktivieren Sie das entsprechende Kontrollkästchen.
6. Klicken Sie auf der Seite zum Auswählen der Komponenten auf die Schaltfläche neben der Komponente ViPNet Business Mail und wählen in der Liste den Eintrag **Wird vollständig auf der lokalen Festplatte installiert** aus. Klicken Sie dann auf **Weiter**.
7. Warten Sie, bis die Installation von ViPNet Business Mail abgeschlossen ist.

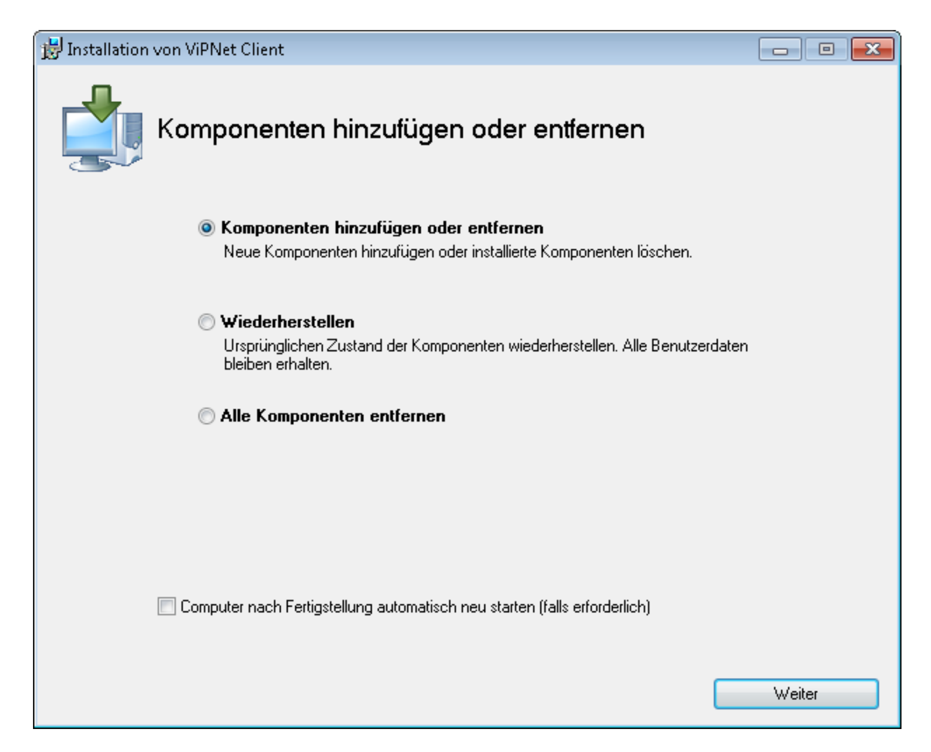


Abbildung 131. Ändern von installierten Komponenten

Klicken Sie dann auf die Schaltfläche **Weiter**.

8 Wenn Sie zuvor den automatischen Neustart des Computers aktiviert haben, dann wird der Computer nun neu gestartet.

Wenn Sie den automatischen Neustart des Computers nicht aktiviert haben, dann klicken im Fenster der Fertigstellung der Installation auf die Schaltfläche **Schließen** und starten den Computer selbständig neu.

Das Programm ViPNet Business Mail ist nun auf dem Client installiert.

Benutzeroberfläche von ViPNet Business Mail

Die Benutzeroberfläche des Programms ViPNet Business Mail ist in der folgenden Abbildung dargestellt:

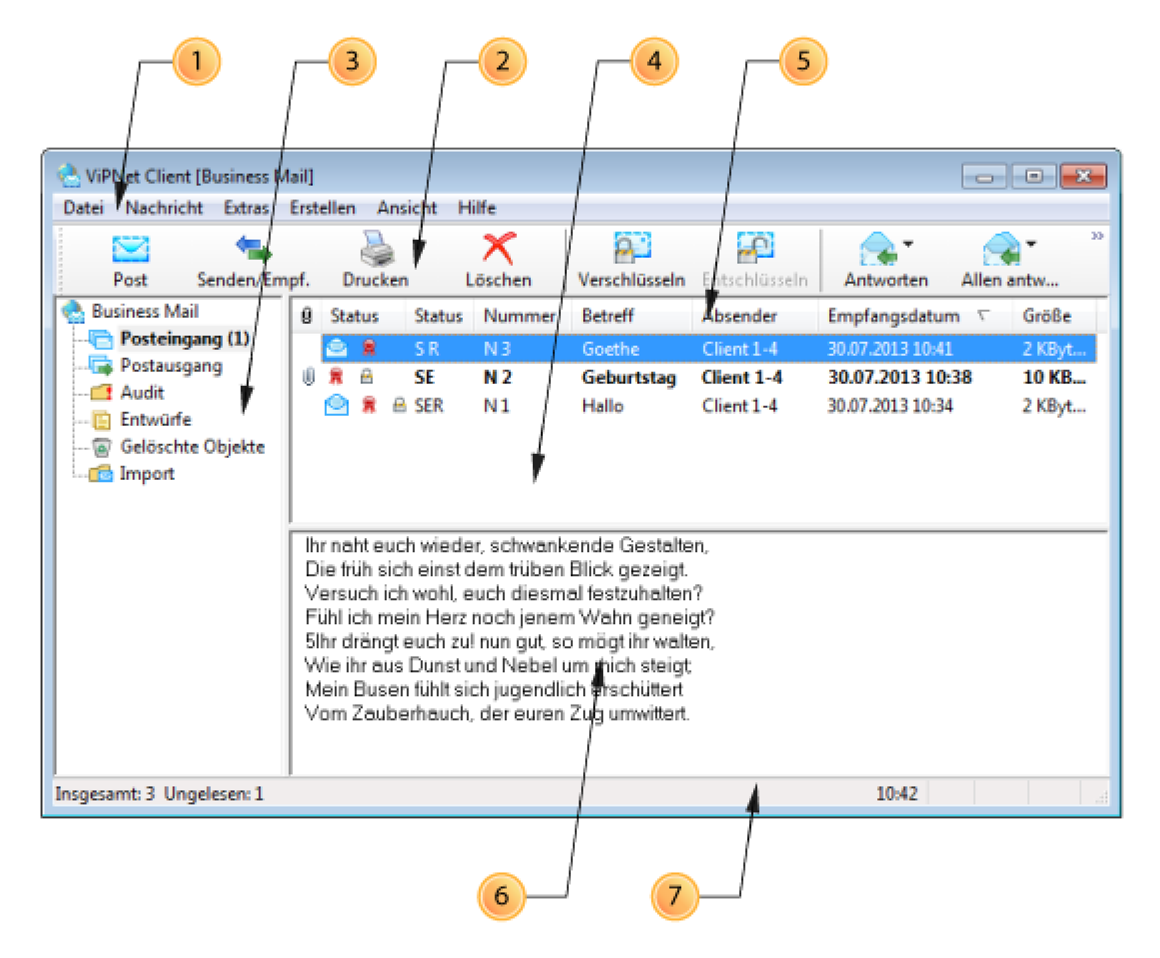


Abbildung 132. Benutzeroberfläche von ViPNet Business Mail

Die Zahlen in der Abbildung kennzeichnen folgende Elemente:

1 Das Hauptmenü des Programms.

2 Die Symbolleiste. Wählen Sie im Menü **Ansicht** den Eintrag **Symbolleiste** und klicken dann auf **Symbolleiste anpassen**, um in der Symbolleiste Schaltflächen hinzuzufügen oder zu entfernen.

3 Der Ordnerbereich. In diesem Bereich wird die Ordnerhierarchie des Programms ViPNet Business Mail abgebildet.

Wenn ein Ordner ungelesene Nachrichten enthält, wird der Ordnername in fetter Schrift dargestellt und die Anzahl der ungelesenen Nachrichten wird in Klammern neben dem Namen des Ordners angezeigt. Wenn ein Ordner weitere Unterordner enthält, die ungelesene Nachrichten enthalten, werden neben dem Ordnername in Klammern zwei Zahlen angezeigt: die Anzahl der ungelesenen Nachrichten im Ordner und die Gesamtanzahl der ungelesenen Nachrichten in allen Unterordnern.

4 Die Nachrichtenliste. Hier wird die Liste aller Nachrichten in dem Ordner angezeigt, der im Ordnerbereich (**3**) ausgewählt ist.

5 Die Spalten der Nachrichtenliste (**4**). In der Spalte **Status** sind die Statussymbole der Nachricht abgebildet.

6 Der Vorschaubereich. In diesem Bereich wird der Brieftext der in der Liste (**4**) ausgewählten Nachricht eingeblendet.

7 Die Statusleiste. In der Statuszeile wird die Gesamtanzahl der Nachrichten im ausgewählten Ordner sowie die Anzahl der ungelesenen (im Ordner **Posteingang**) bzw. nicht zugestellten (im Ordner **Postausgang**) Nachrichten angezeigt.

   Die Anzahl von Nachrichten eines bestimmten Typs wird als Summe zweier Zahlen angezeigt: die Anzahl der Nachrichten dieses Typs im ausgewählten Ordner und die Gesamtanzahl der Nachrichten dieses Typs in allen Unterordnern.

Versenden von Nachrichten

Verfassen der Nachricht

Führen Sie folgende Schritte aus, um eine Nachricht zu verfassen:

1. Klicken Sie im Hauptfenster von ViPNet Business Mail in der Symbolleiste auf die Schaltfläche **Post** . Es wird das Fenster zum Verfassen einer neuen Nachricht geöffnet.
2. Geben Sie im Feld **Betreff** den Betreff der Nachricht ein.
3. Geben Sie im unteren Fensterbereich den Text der Nachricht ein.
4. Wenn Anhänge hinzugefügt werden sollen:
   - Ziehen Sie die Dateien mit der Maus in das Nachrichtenfenster.
   - Klicken Sie in der Symbolleiste auf die Schaltfläche **Anhänge** . Wählen Sie im Fenster **Öffnen** eine oder mehrere Dateien aus.

     Für jede Datei wird das Fenster **Geben Sie den Anhangnamen ein** eingeblendet. Die ausgewählten Dateien werden an die Nachricht angehängt.

   Zum Entfernen der Anhänge:

   - Öffnen Sie im Nachrichtenfenster die Registerkarte **Anhänge**.
   - Wählen Sie die Datei aus, die entfernt werden soll, und drücken die **Entf**-Taste.
5. Wenn die Nachricht verschlüsselt werden soll, klicken Sie in der Symbolleiste auf die Schaltfläche **Verschlüsseln** .
6. So bestimmen Sie die Empfänger der Nachricht:
   - Klicken Sie in der Symbolleiste auf die Schaltfläche **Empfänger** . Es wird das Fenster Adressbuch geöffnet.

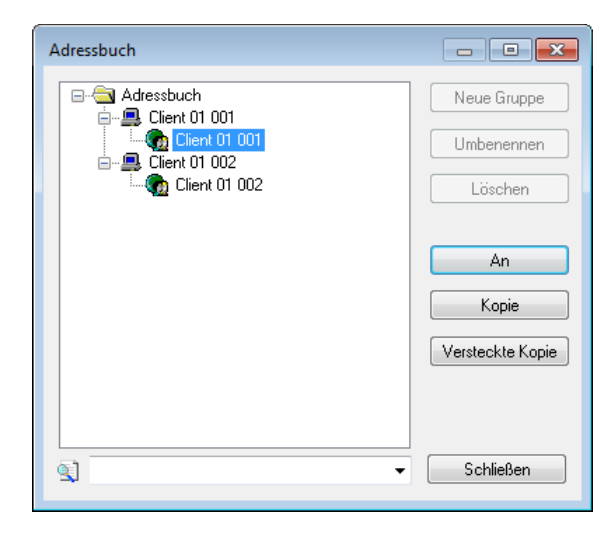


Abbildung 133. Empfänger auswählen

Wählen Sie im Fenster **Adressbuch** einen oder mehrere Empfänger aus und führen eine der folgenden Aktionen durch:

- Klicken Sie auf die Schaltfläche **An**, um die Nachricht an die gewählten Empfänger zu adressieren.
- Klicken Sie auf **Kopie**, um eine Kopie der Nachricht an die gewählten Empfänger zu versenden.
- Klicken Sie auf **Versteckte Kopie**, um eine blinde Kopie der Nachricht an die gewählten Empfänger zu versenden.

Wenn Sie einen Empfänger wieder entfernen möchten, wählen Sie diesen in der Registerkarte **Empfänger** aus und drücken die **Entf**-Taste.

7 Sobald Sie mit dem Verfassen der Nachricht fertig sind, führen Sie inen der folgenden Schritte aus:

- Klicken Sie in der Symbolleiste auf die Schaltfläche **Speichern** oder schließen das Nachrichtenfenster und klicken anschließend im Dialogfeld zum Speichern von Änderungen auf **Ja**, um die Nachricht im Ordner **Postausgang** zu speichern.
- Klicken Sie in der Symbolleiste auf **Senden** , um die Nachricht zu versenden.



Hinweis. Der Statuscode der versendeten Nachricht kann im Ordner **Postausgang** in der Spalte **Status** (s. Benutzeroberfläche von ViPNet Business Mail auf S. 230) abgelesen werden.

Nachrichten digital signieren

Im Programm ViPNet Business Mail können die Nachrichten und Dateien mit Zertifikaten signiert werden, die im Zertifikatspeicher von Windows gespeichert sind (einschließlich RSA-Zertifikate).

Führen Sie die folgenden Schritte aus, um ein solches Zertifikat zu verwenden:

1 Importieren Sie das Zertifikat und den entsprechenden privaten Schlüssel in den Zertifikatspeicher des Systems mit Hilfe des Programms „Zertifikate – aktueller Benutzer“ (certmgr.msc).

   Benutzen Sie die Windows–Hilfe, um weitere Informationen über den Import von Zertifikaten zu erhalten.

2 Stellen Sie sicher, dass im Fenster **Sicherheitseinstellungen** in der Registerkarte **Administrator** das Kontrollkästchen **Benutzung externer Zertifikate erlauben** aktiviert ist.



Hinweis. Die Änderungen der Einstellungen in der Registerkarte **Administrator** können nur vom Netzwerkknoten-Administrator vorgenommen werden

3 Beim Signieren von Nachrichten und Dateien wählen im Menü den punkt **Aktuelles Zertifikat verwenden**.

Das automatische Signieren von Nachrichten und Anhängen mit dem aktuellen Zertifikat ist in „Business Mail“ beim Absenden standardmäßig voreingestellt. Diese Einstellungen können im Bereich **Nachricht** geändert werden.

Führen Sie die folgenden Schritte aus, um eine oder mehrere Nachrichten digital zu signieren:

1 Wählen Sie im ViPNet Business Mail Hauptfenster (s. Benutzeroberfläche von ViPNet Business Mail auf S. 230) im Ordner **Postausgang** (oder einem Unterordner davon) eine oder mehrere ungesendete Nachrichten, die digital signiert werden sollen.

2 Führen Sie einen der folgenden Schritte aus:

   - Klicken Sie in der Symbolleiste auf die Schaltfläche **Signieren** und wählen im Untermenü den Eintrag **Zertifikat auswählen** aus, um Nachrichten mit einem Zertifikat aus einem bestimmten Container des privaten Schlüssels zu signieren.
   - Klicken Sie mit der rechten Maustaste auf die gewählten Nachrichten und wählen im Kontextmenü den Eintrag **Signieren**. Klicken Sie dann auf **Aktuelles Zertifikat verwenden** oder **Zertifikat auswählen**.

   Die Nachrichten werden mit einer digitalen Signatur unterzeichnet und erhalten ein entsprechendes Statusattribut. Wenn die Nachrichten Anhänge enthalten, werden diese ebenfalls signiert.

Führen Sie die folgenden Schritte aus, um eine Nachricht zu signieren, die im Fenster zum Anzeigen und Verfassen von Nachrichten geöffnet ist:

1 Erstellen Sie eine neue Nachricht oder öffnen eine ungesendete Nachricht in einem separaten Fenster.

2 Führen Sie einen der folgenden Schritte aus:

   - Klicken Sie in der Symbolleiste auf die Schaltfläche **Signieren** und wählen im Untermenü den Eintrage **Aktuelles Zertifikat verwenden** aus, um die Nachrichten mit dem Signaturzertifikat des aktuellen Benutzers zu signieren.

- Klicken Sie im Menü Signieren auf den Eintrag **Ganze Nachricht digital signieren** und wählen im Untermenü **Mit aktuellem Zertifikat** oder **Zertifikat auswählen**.

Die Nachricht und ihre Anhänge werden digital signiert.

Senden von Dateien als Anhang

Das Versenden von Dateien als Anhang einer E-Mail-Nachricht ist sehr bequem, in vielen E-Mail-Systemen ist die maximale Größe einer Nachricht jedoch auf 10 MB beschränkt. In ViPNet Business Mail fehlen solche Einschränkungen. Es kann eine beliebige Anzahl von Dateien unbeschränkter Größe an andere ViPNet Benutzer versendet werden. Dabei sollten Sie aber mögliche Einschränkungen in der Geschwindigkeit der Verbindung zum Internet beachten.

Die benötigten Dateien können mit Hilfe der Schaltfläche **Anhänge** während der Erstellung der Nachricht als Anhänge hinzugefügt werden. Ebenso können Dateien in Windows Explorer für den Versand ausgewählt werden. Dazu:

1 Öffnen Sie den Ordner, in dem sich die benötigten Dateien befinden.

2 Wählen Sie eine oder mehrere Dateien aus.

3 Klicken Sie mit der rechten Maustaste auf eine der ausgewählten Dateien und wählen im Kontextmenü den Eintrag **Nachricht senden an ViPNet Empfänger**.

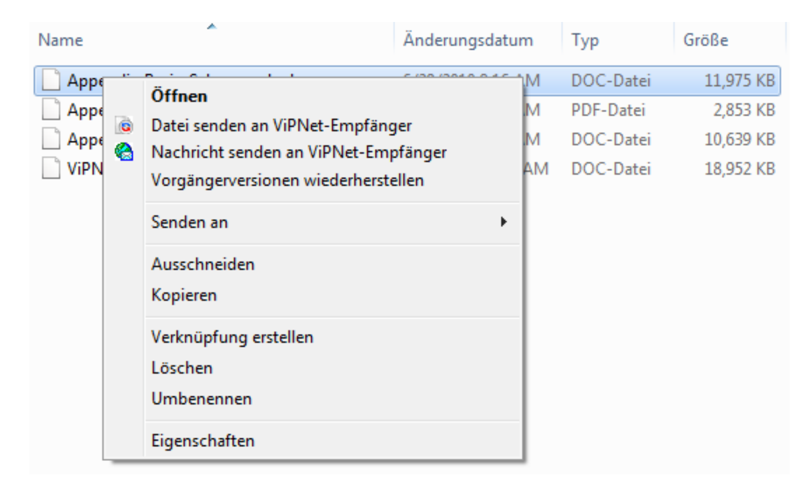


Abbildung 134. Datei als Anhang versenden

4 Geben Sie im Fenster **Geben Sie den Anhangsnamen ein** für jede Datei einen Namen ein. Die ausgewählten Dateien werden an eine neue Nachricht angehängt. Die hinzugefügten Dateien sind im Nachrichtenfenster in der Registerkarte **Anhänge** aufgeführt.

Lesen und Beantworten von Nachrichten

Führen Sie die folgenden Schritte durch, um eine Nachricht zu lesen:

1 Wählen Sie im Hauptfenster von ViPNet Business Mail in der Navigationsleiste den Ordner aus, in dem sich die Nachricht befindet.

2 Wählen Sie die Nachricht aus der Liste. Wenn die E-Mail nicht verschlüsselt ist, wird ihr Text im Bereich unterhalb der Nachrichtenliste eingeblendet.

Wenn die Nachricht verschlüsselt ist, führen Sie zum Anzeigen des Textes einen der folgenden Schritte aus:

- Klicken Sie in der Symbolleiste auf die Schaltfläche **Entschlüsseln** .
- Öffnen Sie die Nachricht mit einem Doppelklick in einem separaten Fenster.

Führen Sie folgende Schritte durch, um eine Nachricht zu beantworten:

1 Wählen Sie die Nachricht in der Liste aus oder öffnen diese mit einem Doppelklick in einem separaten Fenster.

2 Klicken Sie im Hauptfenster von ViPNet Business Mail oder im offenen Nachrichtenfenster in der Symbolleiste auf **Antworten** oder **Allen antworten** .

Es wird das Fenster zum Erstellen einer Nachricht geöffnet.

3 Verfassen und versenden Sie die Nachricht wie im Abschnitt Verfassen der Nachricht (auf S. 232) beschrieben.

Führen Sie einen der folgenden Schritte durch, um eine Nachricht in das Programm Microsoft Outlook oder Outlook Express (Windows Mail) zu übertragen:

- Ziehen Sie die Nachricht aus dem Programmfenster von ViPNet Business Mail in das offene Fenster zum Erstellen einer neuen Nachricht in Microsoft Outlook oder Outlook Express. Die übertragene E-Mail wird in der neuen Nachricht als Anhang eingefügt.
- Ziehen Sie die Nachricht aus dem Programmfenster von ViPNet Business Mail in irgendeinen Ordner im Programmfenster von Microsoft Outlook oder Outlook Express. Im gewählten Ordner wird eine Nachricht eingeblendet, in der die übertragene Business Mail-Nachricht als Anhang eingefügt ist.

Löschen von Nachrichten in ViPNet Business Mail

In manchen Fällen ist es erforderlich, Nachrichten aus den Ordnern des Programms ViPNet Business Mail zu löschen. Dazu:

1 Wählen Sie die Nachricht aus, die gelöscht werden soll, und führen einen der folgenden Schritte aus:

- Klicken Sie mit der rechten Maustaste auf die ausgewählte Nachricht und wählen im Kontextmenü den Eintrag **Löschen**.
- Klicken Sie in der Symbolleiste auf **Löschen** .
- Drücken Sie die **Entf**-Taste.

2 Die gelöschten Nachrichten werden in den Ordner **Gelöschte Objekte** verschoben. Dabei werden im Ordner **Gelöschte Objekte** automatisch Unterordner mit den gleichen Namen erstellt, wie die Namen der Unterordner, aus denen die Nachrichten gelöscht wurden.

3 Wiederholen Sie Schritt **1**, um Nachrichten aus dem Ordner **Gelöschte Objekte** zu entfernen.

Beachten Sie, dass die Nachrichten nie vollständig gelöscht werden können. Nachrichten, die aus dem Ordner **Gelöschte Objekte** gelöscht wurden, werden in den Ordner **Audit** verschoben. Zum Entfernen der Nachrichten im Ordner **Audit** sollte sich der Benutzer als Administrator in ViPNet Business Mail anmelden. Dazu:

1. Wählen Sie im Menü **Extras** den Eintrag **Sicherheitseinstellungen**.
2. Klicken Sie im Fenster **Sicherheitseinstellungen** auf die Registerkarte **Administrator**.
3. Klicken Sie auf die Schaltfläche **Administrator-Login** und geben das Passwort des ViPNet Netzwerkknoten-Administrators ein.



Beginn der Arbeit mit dem Programm ViPNet Coordinator für Windows

Funktionen des Coordinators im ViPNet Netzwerk

In der Regel übernimmt der Coordinator innerhalb des Netzwerks eine oder mehrere Funktionen in Abhängigkeit davon, welche Aufgaben im Rahmen des Firmennetzwerks, seiner Struktur, der Auslastung des Coordinators u. s. w. gelöst werden müssen. Die Funktionalität des Coordinators kann folgende Bereiche umfassen:

- Funktionen eines Mail-Servers für die Nachrichten des Programms Business Mail und die Dienstmeldungen von ViPNet Network Manager (Kommunikationsserver).
- Benachrichtigung der Netzwerkknoten über die Zugangsparameter der Knoten zueinander (IP-Adressenserver).
- Proxy-Funktion für den geschützten Datenverkehr (Aufbau verschlüsselter Verbindungen zwischen geschützten Netzwerken über öffentliche Netzwerke).
- Filterung des unverschlüsselten und des getunnelten Traffics (Firewall).
- Aufbau geschützter Verbindungen zu offenen Objekten im lokalen Netzwerk (Tunnelung).
- Dynamische und statische Umsetzung der IP-Adressen (NAT).
- Sicherstellung von IPsec-Verbindungen mit Smartphone-Clients.

IP-Adressenserver

Bei der Einbindung eines Clients mit ViPNet Client in das Netzwerk oder bei einer Änderung seiner Verbindungsparameter werden diese Parameter an den Coordinator weitergeleitet, der die Rolle eines IP-Adressenservers für den gegebenen Computer erfüllt. Der IP-Adressenserver sendet an den Client seinerseits Daten über Status und Verbindungsparameter aller anderen Knoten, mit denen der Client verbunden ist.

Auf diese Weise erfüllt der IP-Adressenserver die folgenden Funktionen:

- Empfang von Statusinformationen der Clients;
- Bereitstellung von Informationen über den Status und die Zugangsparameter für diejenigen Netzwerkknoten, mit denen der aktuelle Client verbunden ist.



Abbildung 135. Role des IP-Adressenservers im ViPNet-Netzwerk

Die Auflistung aller Netzwerkknoten, die mit dem Computer verbunden sind, sowie ihre Zugangsparameter werden im Programm ViPNet Monitor im Bereich **Privates Netzwerk** angezeigt.

Ein Client sendet in vorgegebenen Zeitintervallen (standardmäßig alle 5 Minuten) Statusinformationen an seinen Coordinator, um seine Anwesenheit im Netzwerk zu bestätigen. Wenn keine Nachricht vom Client eingeht, wird er vom Coordinator mit dem Status „Unerreichbar“ versehen.

Standardmäßig tritt für einen Client sein Kommunikationsserver (Coordinator, auf dem der Client im Programm ViPNet Network Manager registriert ist) als IP-Adressenserver auf. Im Gegensatz zum Kommunikationsserver kann der IP-Adressenserver auch gewechselt werden, indem ein anderer Coordinator, zu dem eine Verbindung besteht, als IP-Adressenserver ausgewählt wird.

Kommunikationsserver

Im ViPNet ist jeder Client einem Coordinator zugeordnet, welcher als sein Kommunikationsserver agiert. Die Zuordnung erfolgt im ViPNet Network Manager und kann weder auf dem Coordinator noch auf dem Client geändert werden.

Das Routing von Nutz- und Steuerungsdaten wird mit Hilfe des Transportmoduls ViPNet MFTP durchgeführt, welches in der Anwendungsschicht aktiv ist. Das MFTP-Modul auf dem Coordinator empfängt die Daten anderer ViPNet Netzwerkknoten und leitet diese an den jeweiligen Zielknoten weiter.

Das Routing von Daten zwischen den Coordinatoren wird auf Basis von serverübergreifenden Kanälen, die für diese Coordinatoren eingerichtet sind, durchgeführt. Die serverübergreifenden Kanäle können nach beliebigem Schema organisiert werden. Wenn es mehrere Routen zur Datenübermittlung zwischen den Coordinatoren gibt, dann wird die kürzeste Route für die Übertragung der Daten gewählt. Die Übermittlung von Daten von einem Netzwerk in ein anderes Netzwerk erfolgt über Gateway-Coordinatoren, die für eine effektive Partnernetzwerk-Kommunikation zwischen den beiden Netzwerken sorgen.



Abbildung 136. Aufgaben eines Kommunikationsservers im ViPNet-Netzwerk

Beim Eintreffen einer Anwendungs- oder Steuerungsdatei legt der Kommunikationsserver in Übereinstimmung mit den Routingtabellen den weiteren Weg zur Übermittlung dieser Datei fest. Wenn es sich um eine Multicast-Datei handelt, wird sie vom Server in entsprechende Einzelteile zerlegt. Nachdem der Kommunikationsserver die Datei erhalten hat, führt er in Abhängigkeit von vorgegebenen Parametern einen der folgenden Schritte durch:

- Er baut eine Verbindung zum Netzwerkknoten auf (standardmäßig wird diese Logik dann angewendet, wenn die Datei an einen anderen Kommunikationsserver weitergeleitet werden soll).
- Er wartet, bis eine Verbindung vom Dateiempfänger aufgebaut wird (standardmäßig wird diese Logik dann angewendet, wenn Dateien für Clients eingetroffen sind).

Es kann für andere Objekte eine Abfrageperiode festgelegt werden unabhängig davon, für welches Objekt die Pakete bestimmt sind. Wenn die Verbindung unterbrochen und wieder aufgebaut wird, erfolgt die Datenübertragung von der Unterbrechungsstelle, was vor allem bei Einwahlverbindungen besonders vorteilhaft ist.

Router der VPN-Pakete

Zu den wichtigsten Funktionen des Coordinators gehört der Schutz von vertraulichen Daten bei der Übertragung von einem ViPNet Netzwerk in ein anderes über ungesicherte Verbindungskanäle. Der Coordinator eines ViPNet Netzwerks gewährleistet dabei eine sichere Verbindung zum Coordinator des anderen ViPNet Netzwerks.



Abbildung 137. Coordinator als Router im ViPNet Netzwerk

Das Routing des verschlüsselten Traffics wird anhand der Identifikatoren der geschützten Knoten, die im offenen, vor Fälschungen geschützten Teil des IP-Pakets enthalten sind, sowie anhand des geschützten dynamischen Routing-Protokolls für den VPN-Traffic durchgeführt. Parallel dazu wird die Netzwerkadressenübersetzung (NAT) (auf S. 371) für den verschlüsselten Traffic durchgeführt. Alle geschützten Transit-Pakete, die auf dem Coordinator eintreffen, werden im Namen der IP-Adresse des

Coordinators an andere Knoten weitergeleitet. Die Netzwerkadressenübersetzung für den geschützten Traffic wird in Übereinstimmung mit Parametern, die nicht geändert werden können, automatisch durchgeführt.

Wenn sich an der Grenze des ViPNet Netzwerks irgendein Drittgerät befindet, das die Filterung und die Adressenübersetzung für den weitergeleiteten Traffic durchführt, dann kann der Coordinator in diesem Fall die Rolle des Verbindungsservers übernehmen. Mit Hilfe eines Verbindungsservers können die Clients Verbindungen zueinander aufbauen, falls direkte Verbindungen zwischen den Clients nicht möglich sind. Für jeden Client kann ein eigener Verbindungsserver ausgewählt werden. Standardmäßig wird der IP-Adressenserver als Verbindungsserver für die Clients festgelegt.



Abbildung 138. Aufbau der Verbindung zwischen ViPNet-Netzwerkknoten

Firewall

Der Coordinator führt die Filterung offener IP-Pakete auf jedem Netzwerkadapter nach IP-Adresse, Protokoll und Port in Übereinstimmung mit den konfigurierten Netzwerkfiltern durch (s. Grundprinzipien der Traffic-Filterung auf S. 271). Mit Hilfe der Netzwerkfilter können nicht nur unerwünschte Verbindungen blockiert, sondern auch Verbindungen zu offenen Knoten außerhalb des ViPNet Netzwerks erlaubt werden.

Neben den konfigurierbaren Filtern verfügt das Programm auch über ein Antispoofing-System. Dieses System schützt den Computer vor einem der verbreiteten Arten von Netzwerkangriffen.



Abbildung 139. Rolle der Firewall im ViPNet-Netzwerk

Der Coordinator kann außerdem die Netzwerkadressenübersetzung (NAT) für den durchlaufenden offenen Traffic durchführen (s. Netzwerkadressenübersetzung (NAT) auf S. 371).



Hinweis. Die Netzwerkadressenübersetzung für den verschlüsselten Traffic wird automatisch durchgeführt (s. Router der VPN-Pakete auf S. 241).

Die NAT-Funktionalität für den offenen Traffic ermöglicht die Konfiguration von Regeln der Adressenübersetzung, wodurch zwei grundlegende Aufgaben gelöst werden:

- Anbindung des lokalen Netzwerks an das Internet, wenn die Anzahl der lokalen Netzwerkknoten die vom Internetdienstanbieter zur Verfügung gestellte Anzahl an öffentlichen IP-Adressen übersteigt. Auf diese Weise wird es Computern mit lokalen IP-Adressen ermöglicht, den Zugang zum Internet im Namen der öffentlichen IP-Adresse des Coordinators zu erhalten.

  Zur Lösung dieser Aufgabe wird die Quell-Adressenübersetzung verwendet.
- Einrichtung des Zugangs externer Teilnehmer zu internen Ressourcen. Durch Verwendung der NAT-Technologie können Knoten des lokalen Netzwerks, die über private IP-Adressen verfügen, für Internetbenutzer über öffentliche IP-Adressen zugänglich sein.

  Zur Lösung dieser Aufgabe wird die Ziel-Adressenübersetzung verwendet.

VPN-Gateway

Das VPN-Gateway ermöglicht es, offene Knoten in das geschützte ViPNet Netzwerk einzubinden, ohne dass ViPNet Software auf diesen Knoten installiert werden muss. Zusätzlich hilft das VPN-Gateway, Verbindungen unter Beteiligung offener Knoten bei Datenübertragung über das Internet oder andere öffentliche Netzwerke zu schützen. Für die Lösung dieser Aufgaben wird die Technologie der Tunnelung verwendet (s. Schutz des Traffics offener Netzwerkknoten (Tunnelung) auf S. 299).

Die Tunnelung besteht in der Verschlüsselung des Traffics offener Knoten durch den Coordinator, der als VPN-Gateway auftritt. Mit Hilfe der Technologie der Tunnelung können geschützte Verbindungen zwischen offenen Knoten und geschützten ViPNet Knoten oder zwischen zwei offenen Knoten, die von unterschiedlichen Coordinatoren getunnelt werden, hergestellt werden.

Die Tunnelung ermöglicht den effektiven Schutz des Traffics jener Knoten, auf denen die Software ViPNet Client oder ViPNet Coordinator nicht installiert werden kann. Dabei kann es sich zum Beispiel um unterschiedliche Server, Apple-Computer, Netzwerkdrucker, Netzwerkspeicher u. s. w. handeln.

Der Schutz des Traffics offener Knoten bei Verwendung der Tunnelung wird auf die folgende Weise sichergestellt:

- Offene IP-Pakete werden vom getunnelten Knoten zum Coordinator geleitet.
- Auf dem Coordinator werden die IP-Pakete durch Netzwerkfilter verarbeitet, verschlüsselt und an den geschützten Knoten, der als Ziel dieser Pakete festgelegt ist, oder an einen anderen Coordinator weitergeleitet.
- Wenn auf dem Coordinator verschlüsselte IP-Pakete eintreffen, die für einen getunnelten Knoten bestimmt sind, dann werden diese IP-Pakete durch Netzwerkfilter verarbeitet, entschlüsselt und offen an den Zielknoten weitergeleitet.



Abbildung 140. Tunnelung im ViPNet Netzwerk

Damit der Coordinator die Tunnelung durchführen kann, sollten im Programm ViPNet Network Manager oder unmittelbar auf dem Coordinator die IP-Adressen der getunnelten Geräte definiert werden (s. Konfiguration der Tunnelung auf S. 302).

TCP-Tunnel

Wenn Verbindungen über das UDP-Protokoll nicht unterstützt werden, kann auf dem Coordinator ein TCP-Tunnel konfiguriert werden. Über diesen Tunnel werden Verbindungen zwischen den ViPNet Netzwerkknoten unter Verwendung des TCP-Protokolls hergestellt. In der Regel ist der Versand von UDP-Paketen bei Remoteverbindungen zum ViPNet Netzwerk über ein NAT-Gerät nicht möglich.



Abbildung 141. Funktionen eines TCP-Tunnels

Wenn sich ein Knoten nicht über das UDP-Protokoll mit dem Coordinator verbinden kann, und wenn auf dem Coordinator dabei ein TCP-Tunnel eingerichtet ist, dann stellt der Knoten automatisch eine Verbindung über das TCP-Protokoll mit dem Coordinator her. Die übermittelten TCP-Pakete werden vom Coordinator in UDP-Pakete umgewandelt und dann an den Zielknoten weitergeleitet.

Vor Beginn der Arbeit mit dem Programm ViPNet Coordinator

Führen Sie vor Beginn Ihrer Arbeit mit dem Programm ViPNet Coordinator Monitor die Schritte aus der nachfolgenden Tabelle aus.

Tabelle 15. Vorbereitung der Arbeit mit ViPNet Coordinator Monitor

	Aktion	Verweis
☐	Installieren Sie eine ViPNet Schlüsseldistribution auf den Computer	Installation der Schlüsseldistribution (auf S. 216)
☐	Starten Sie das Programm ViPNet Monitor	Start des Programms ViPNet Monitor (auf S. 217)
☐	Konfigurieren Sie die Netzwerk-Verbindungsparameter, sofern diese Parameter nicht bereits im Programm ViPNet Network Manager konfiguriert wurden	Konfiguration der Netzwerkverbindung der Coordinatoren (auf S. 251)
☐	Konfigurieren Sie den Zugang zu geschützten und getunnelten Knoten	Konfiguration des Zugangs zu geschützten Netzwerkknoten (auf S. 262) Konfiguration des Zugangs zu getunnelten Netzwerkobjekten (auf S. 265)
☐	Konfigurieren Sie die Firewallparameter	Integrierte Firewall (auf S. 269)
☐	Konfigurieren Sie die Adressenübersetzung (NAT)	Übersetzung von IP-Adressen (NAT) (auf S. 285)
☐	Konfigurieren Sie die Verarbeitungsparameter für die Netzwerkprotokolle	Bearbeitung der Anwendungsprotokolle (auf S. 293)
☐	Konfigurieren Sie die Tunnelung	Konfiguration der Tunnelung (auf S. 302)
☐	Konfigurieren Sie die DNS- und WINS-Namensdienste	Konfiguration und Verwendung der Namensdienste DNS und WINS im ViPNet Netzwerk (auf S. 305)

Nach der Durchführung aller erforderlichen Schritte und Einstellungen wird der Coordinator die Verbindungen zwischen den Netzwerkknoten sicherstellen und seine anderen Funktionen innerhalb des geschützten ViPNet Netzwerks erfüllen.

Im Programm ViPNet Coordinator Monitor können Sie zusätzlich die folgenden Aktionen durchführen:

- Mit der Liste der geschützten Knoten (s. Arbeiten mit der ViPNet Netzwerkknotenliste auf S. 220) arbeiten;
- Nachrichten mit den Benutzern anderer Netzwerkknoten austauschen (s. Verschlüsselter Chat auf S. 222);
- Dateien austauschen (s. Empfang von Dateien auf S. 223);
- Updates mit Hilfe des ViPNet Updatesystems (s. Empfang von Updates auf S. 224) annehmen und installieren.

Benutzerinterface von ViPNet Coordinator

Das Hauptfenster des Programms ViPNet Coordinator Monitor ist unten dargestellt:

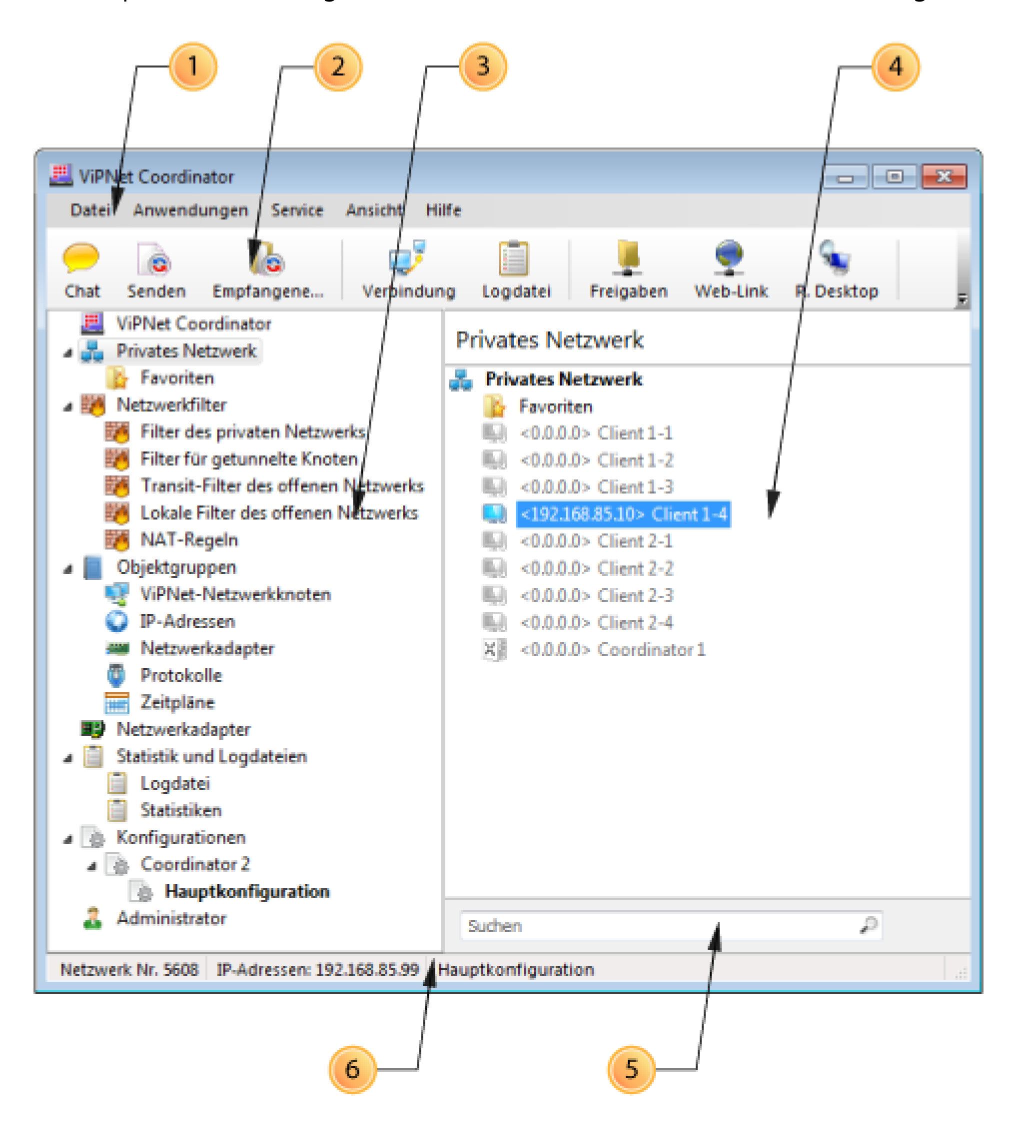


Abbildung 142. Programmfenster ViPNet Monitor

Mit den Zahlen 1 bis 6 sind gekennzeichnet:

1. Das Hauptmenü des Programms.
2. Die Symbolleiste. Um Symbole anzeigen oder verstecken, wählen Sie die Option **Symbolleiste** im Menü **Ansicht** aus. Ebenso können Sie die Schaltflächen in der Symbolleiste mit Hilfe der Schaltfläche . Ziehen Sie zum Ändern der Schaltflächenpositionen in der Symbolleiste die betroffene Schaltfläche auf die gewünschte Stelle, während Sie die **ALT**-Taste gedrückt halten.

3 Navigationsleiste enthält die Liste aller Bereiche, die zur Einstellung verschiedener Parameter von ViPNet Monitor dient:

- **Privates Netzwerk** (standardmäßig ist dieser Bereich ausgewählt). Dieser enthält die Liste aller ViPNet-Netzwerkknoten, die mit dem eigenen Netzwerkknoten verbunden sind. Diese Verbindungen werden in ViPNet Network Manager bestimmt. Mehr Informationen finden Sie im Abschnitt Arbeiten mit der ViPNet Netzwerkknotenliste (auf S. 220).
- **Netzwerkfilter**. Enthält Unterbereiche mit Filter für den IP-Traffic:
  - **Filter des privaten Netzwerks**: dient zum Konfigurieren der Filter für den verschlüsselten Traffic.
  - Filter getunnelte Knoten: dient zum Einstellen der Traffic-Filter für getunnelte Knoten (s. Schutz des Traffics offener Netzwerkknoten (Tunnelung) auf S. 299).
  - **Transit-Filter des offenen Netzwerks**: dient zum Einstellen von Transit-Filter.
  - **Lokale Filter des offenen Netzwerks**: dient zum Einstellen von lokalen Filter des offenen Netzwerks.
  - **NAT-Regeln**: dient zum Einstellen der Regeln für Umsetzung der IP-Adressen für öffentliche Netzwerke (s. Übersetzung von IP-Adressen (NAT) auf S. 285).
- **Objektgruppen**: enthalten Listen von Objekten, die zum Erstellen von Netzwerkfiltern verwendet werden können: ViPNet Netzwerkknoten-Gruppen, IP-Adressgruppen, u. s. w.
- **Netzwerkadapter**: enthält eine Liste des Netzwerkadapter, die auf dem Computer installiert sind.
- **Statistik und Logdateien.** Enthält folgende Unterbereiche:
  - **Logdatei**: dient der Anzeige von Einträgen der IP-Paketlogdatei (s. Verwendung der Logdatei auf S. 324).
  - **Statistiken**: dient zur Anzeige von Statistiken über IP-Paketfilterung.
- **Konfigurationen**: dient der Verwaltung von Konfigurationen von ViPNet Network Manager (s. Steuerung von Programmkonfigurationen auf S. 331).
- **Administrator**: wird nur nach der Anmeldung im Programm im Administratormodus angezeigt und dient der Einstellung von erweiterten Programmparametern (s. Arbeiten mit Administratorrechten auf S. 338).

4 In der Panel-Ansicht wird der Inhalt des ausgewählten Menüpunktes (**3**) angezeigt.

5 Das Suchfeld wird in den Bereichen **Privates Netzwerk**, **Netzwerkfilter** und **Objektgruppen** angezeigt. Für eine Suche innerhalb eines Bereichs tragen Sie im Suchfeld einen Teil des Pfades oder des Namens sowie ggf. andere Parameter des Netzwerkknotens ein.

Im Bereich **Privates Netzwerk** wird anhand der folgenden Parameter gesucht:

- Netzwerkknoten (wird im Bereich **Privates Netzwerk** und im Fenster **Netzwerkknoten-Eigenschaften** in der Registerkarte **Allgemeine** angezeigt).
- Computername (das Fenster **Netzwerkknoten-Eigenschaften**, die Registerkarte **Allgemeine**).
- Alias (das Fenster **Netzwerkknoten-Eigenschaften**, die Registerkarte **Allgemeine**).

- Reelle und virtuelle IP-Adresse (das Fenster **Netzwerkknoten-Eigenschaften**, die Registerkarte **IP-Adressen**, die Liste **IP-Adressen**).
- DNS-Name (das Fenster **Netzwerkknoten-Eigenschaften**, die Registerkarte **IP-Adresse**, die Liste **DNS-Name**).
- Netzwerkknoten-ID (das Fenster **Netzwerkknoten-Eigenschaften**, die Registerkarte **Allgemeine**).

Um das Suchfeld zu leeren, klicken Sie auf **Alle anzeigen**.

6 Statusleiste. Enthält die folgende Informationen: ViPNet Netzwerknummer, IP-Adressen, die dem Netzwerkknoten zugeordnet sind, und die aktuelle Konfiguration des Programms. Wählen Sie zum Ein- oder Ausblenden der Statusleiste im Menü **Ansicht** den Eintrag **Statusleiste**.



Konfiguration der Netzwerk-Verbindungsparameter und Parameter der Zugang zu geschützten Netzwerkknoten

Konfiguration der Netzwerkverbindung der Coordinatoren

Die auf den Coordinatoren vorzunehmenden Einstellungen hängen von der erforderlichen Funktionalität dieser Netzwerkknoten sowie von den Parametern, die im Programm ViPNet Network Manager konfiguriert wurden, ab (s. Vorgehensweise beim Konfiguration des ViPNet Netzwerks auf S. 107).

Wenn alle erforderlichen Coordinatoreinstellungen (IP-Adressen, Firewallparameter, Adressen getunnelter Knoten) im Programm ViPNet Network Manager vorgenommen wurden, dann sind keine weiteren Einstellungen auf den Netzwerkknoten notwendig. Die IP-Adressen der Coordinatoren und der getunnelten Knoten werden auf den anderen Coordinatoren und Clients automatisch übernommen.

Wenn die erforderlichen Einstellungen nicht im Programm ViPNet Network Manager vorgenommen wurden, dann sollte diese manuell im Programm ViPNet Monitor auf jedem einzelnen Netzwerkknoten durchgeführt werden.

Wenn sich der Coordinator hinter einer Firewall befindet, die an der Grenze des lokalen Netzwerks eingerichtet ist und statische Netzwerkadressenübersetzung durchführt, dann sollten einige zusätzliche Einstellungen auf dieser Firewall konfiguriert werden (s. Verbindung über eine Firewall mit der statischen Umsetzung von IP-Adressen auf S. 255).

Weitere Informationen über mögliche Typen von Verbindungen im ViPNet Netzwerk finden Sie in der Dokument „Grundsätze beim Aufbau von Verbindungen im ViPNet Netzwerk. Allgemeine Informationen".

Verbindung ohne Firewall

Dieser Verbindungstyp sollte dann auf dem Coordinator ausgewählt werden, wenn kein einziger Netzwerkadapter dieses Coordinators mit einem NAT-Gerät verbunden ist, d. h. wenn der Coordinator aus dem gerouteten Netzwerk erreichbar ist. Wenn der Coordinator auch für Knoten in externen Netzwerken erreichbar sein soll, dann sollte zumindest ein Netzwerkadapter auf diesem Coordinator über eine öffentliche IP-Adresse verfügen.

Führen Sie die folgenden Schritte aus, um Verbindungen ohne Verwendung einer Firewall zu konfigurieren:

1 Wählen Sie im Programmfenster von ViPNet Monitor im Menü **Service** den Eintrag **Anwendungseinstellungen**.

2 Wählen Sie im Fenster **Einstellungen** in der Navigationsleiste den Bereich **Privates Netzwerk**.

3 Deaktivieren Sie das Kontrollkästchen **Externe Firewall verwenden**, um eine Verbindung ohne Verwendung der Firewall auf dem Coordinator zu konfigurieren.

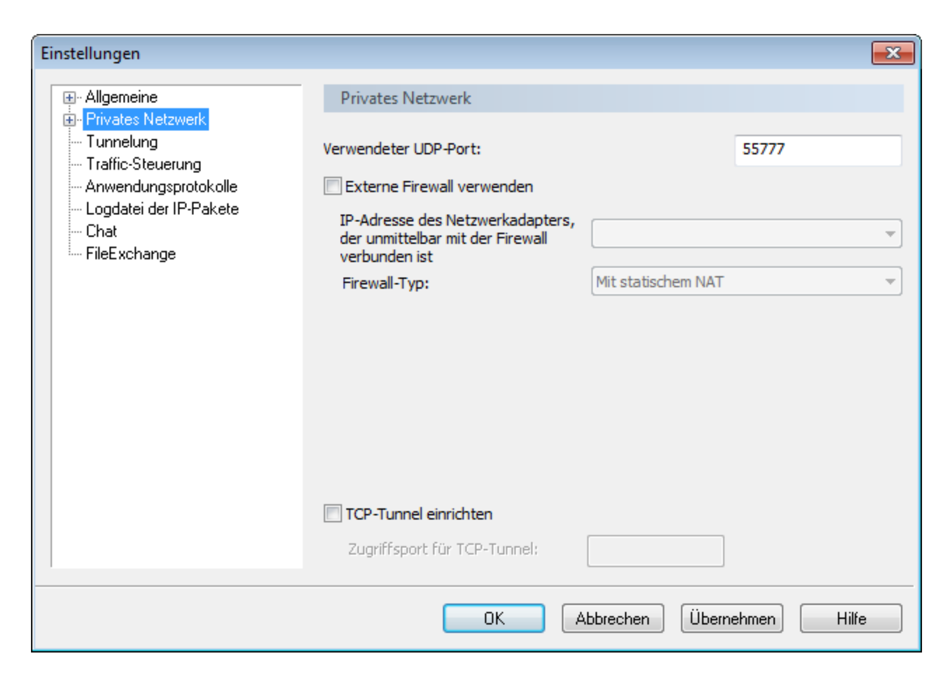


Abbildung 143. Verbindung des Coordinators ohne Verwendung einer Firewal

Deaktivieren Sie das Kontrollkästchen **Firewall verwenden**, um eine Verbindung ohne Verwendung der Firewall auf dem Client zu konfigurieren.

4 Klicken Sie auf die Schaltfläche **Übernehmen**, um die Einstellungen zu speichern.

Verbindung über einen Coordinator

Wenn an der Grenze des lokalen Netzwerks ein ViPNet Coordinator als Gateway aufgestellt ist, dann wird es empfohlen, diesen Coordinator als Firewall für die Clients des lokalen Netzwerks zu konfigurieren. In diesem Fall wird der gesamte verschlüsselte Traffic zwischen diesem Client und den Knoten des externen Netzwerks über den Coordinator geleitet. Der Coordinator übernimmt auf diese Weise die Rolle eines Routers für verschlüsselte Pakete, mit eingebauter Funktion der Adressenübersetzung.

Zum Einstellen der Verbindung über einen anderen Coordinator:

1 Wählen Sie im Programmfenster von ViPNet Monitor im Menü **Service** den Eintrag **Anwendungseinstellungen** aus.

2 Wählen Sie im Fenster Einstellungen in der Navigationsleiste den Bereich **Privates Netzwerk** aus.

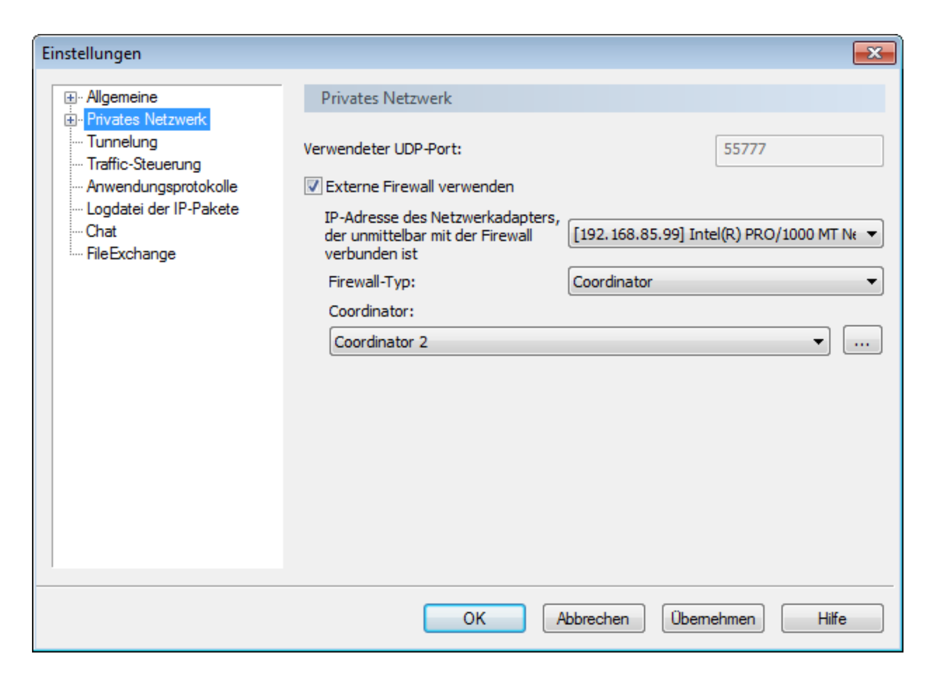


Abbildung 144. Verbindung eines Coordinators über einen anderen Coordinator

3 Aktivieren Sie das Kontrollkästchen **Firewall verwenden** (in ViPNet Client) oder **Externe Firewall verwenden** (in ViPNet Coordinator).

4 Wählen Sie den Eintrag **Coordinator** in der Liste **Firewall-Typ** aus.

5 Wenn Sie das Programm ViPNet Coordinator konfigurieren, wählen Sie in der Liste **IP-Adresse des Netzwerkadapters, der unmittelbar mit der Firewall verbunden ist** den Netzwerkadapter aus, über den die Verbindung zu dem Coordinator erfolgen soll, der als Firewall agiert.

6 Wählen Sie in der Liste **Coordinator** den Coordinator aus, der als Firewall verwendet werden soll.

Wenn Sie das Programm ViPNet Client konfigurieren, wird als Firewall standardmäßig der Coordinator ausgewählt, der als VPN-Server eingestellt wurde. Bei Bedarf können Sie auch einen anderen Coordinator auswählen. Zum Beispiel, mobile ViPNet Benutzer können in verschiedenen Netzwerken unterschiedliche Coordinatoren benutzen.

7 Klicken Sie auf **OK**.

Verbindung über eine Firewall mit der dynamischen Umsetzung von IP-Adressen

Für den Schutz des Traffics lokaler Netzwerkknoten ist es ratsam, einen ViPNet Coordinator als Firewall zu verwenden. Wenn sich an der Grenze des lokalen Netzwerks eine Firewall oder ein anderes Gerät befindet, das die Adressenübersetzung (NAT) durchführt, und wenn dabei das Einstellen statischer NAT-Regeln auf diesem Gerät nur schwer möglich ist, dann sollte ein Coordinator zwischen diesem NAT-Gerät und den Knoten des lokalen Netzwerks aufgestellt werden. Auf dem Netzwerkadapter des Coordinators, der mit dem NAT-Gerät verbunden ist, sollte die Verbindung über eine Firewall mit dynamischer Adressenübersetzung konfiguriert werden. Zusätzlich sollte dieser Coordinator für alle ViPNet Clients des lokalen Netzwerks als Firewall festgelegt werden.



Abbildung 145. Verbindung über eine Firewall mit dynamischem NAT

Für den Client sollte dieser Verbindungstyp dann ausgewählt werden, wenn sich im lokalen Netzwerk kein Coordinator befindet, der als Firewall eingesetzt werden kann, und dabei alle Verbindungen zum externen Netzwerk über eine Firewall geleitet werden, auf der keine statischen NAT-Regeln konfiguriert werden können.

Damit Verbindungen über eine Firewall mit dynamischem NAT ordnungsgemäß aufgebaut werden, sollte sich im externen Netzwerk ein Coordinator befinden, der über eine öffentliche IP-Adresse zugänglich ist. Die IP-Adresse der verwendeten Firewall sollte in den Netzwerkeinstellungen des Betriebssystems auf dem geschützten Knoten als Standardgateway festgelegt werden.

Zum Einstellen von Verbindungen über eine Firewall mit dynamischem NAT:

1. Wählen Sie im Programmfenster von ViPNet Monitor im Menü **Service** den Eintrag **Anwendungseinstellungen** aus.
2. Wählen Sie im Fenster **Einstellungen** in der Navigationsleiste den Bereich **Privates Netzwerk** aus.
3. Aktivieren Sie das Kontrollkästchen **Firewall verwenden** (in ViPNet Client) oder **Externe Firewall verwenden** (in ViPNet Coordinator verwenden).
4. Wenn Sie das Programm ViPNet Coordinator konfigurieren, wählen Sie in der Liste **Firewall-Typ** die Option **Mit dynamischem NAT** aus.

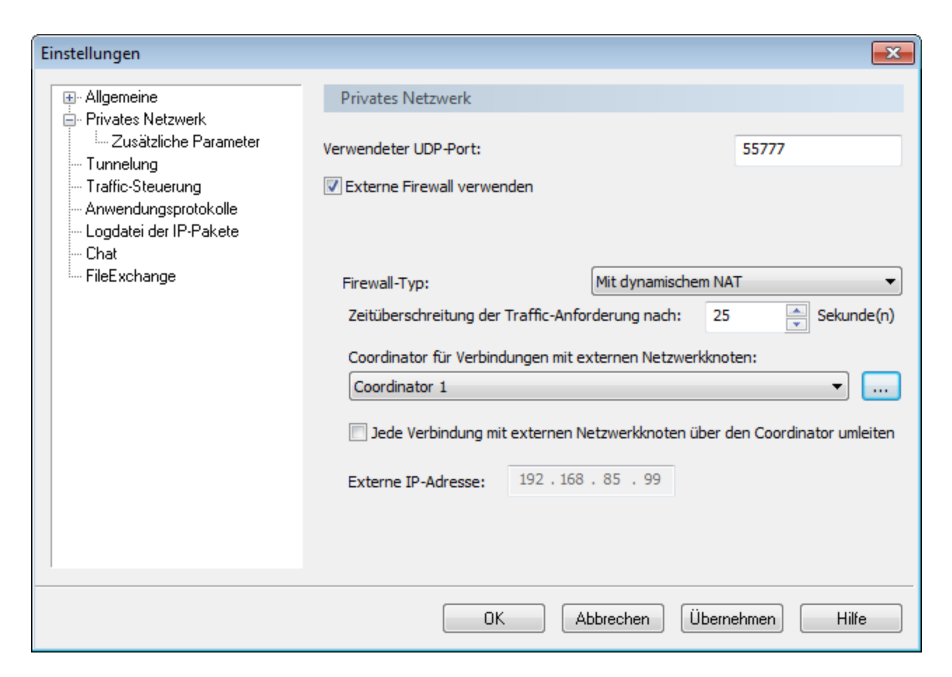


Abbildung 146. Verbindung eines Coordinators über eine Firewall mit dynamischem NAT

5 Wählen Sie den Coordinator der eingehenden Verbindungen in der Liste **Coordinator für Verbindungen mit externen Netzwerkknoten** aus. Dieser Coordinator soll entweder direkt oder über eine Firewall mit statischem NAT erreichbar sein.

Damit die Verbindung im aktiven Zustand bleibt, sendet der Netzwerkknoten regelmäßig UDP-Pakete an seinen Coordinator der eingehenden Verbindungen. Standardmäßig beträgt das Sendeintervall 25 Sekunden. Bei Bedarf kann dieser Wert im Feld **Zeitüberschreitung der Traffic-Anforderung nach** geändert werden. Das festgelegte Intervall darf die Lebensdauer der dynamischen Regel auf dem NAT-Gerät nicht übersteigen.

6 Aktivieren Sie das Kontrollkästchen **Jede Verbindung mit externen Netzwerkknoten über den Coordinator umleiten**, wenn der gesamte ein- und ausgehende Traffic über den Coordinator für eingehende Verbindungen geleitet werden soll.



Hinweis. Falls das Kontrollkästchen aktiviert ist, kann das zu einer wesentlichen Minderung der Übertragungsrate führen. Deswegen sollte dieser Modus nur in besonderen Fällen verwendet werden.

7 Klicken Sie auf die Schaltfläche **Übernehmen**, um die Einstellungen zu speichern.

Verbindung über eine Firewall mit der statischen Umsetzung von IP-Adressen

Wenn an der Grenze des lokalen Netzwerks zum externen Netzwerk eine Firewall aufgestellt ist, die die Übersetzung von Netzwerkadressen (NAT) durchführt und auf welcher statische Regeln der Adressenübersetzung definiert werden können, dann sollte zwischen dieser Firewall und den Knoten des lokalen Netzwerks ein Coordinator eingerichtet werden. Auf dem Coordinator sollten in diesem Fall die

Parameter der Verbindungen über eine Firewall mit statischem NAT konfiguriert sein. Für die Clients des lokalen Netzwerks sollte der gegebene Coordinator als Verbindungsserver verwendet werden.

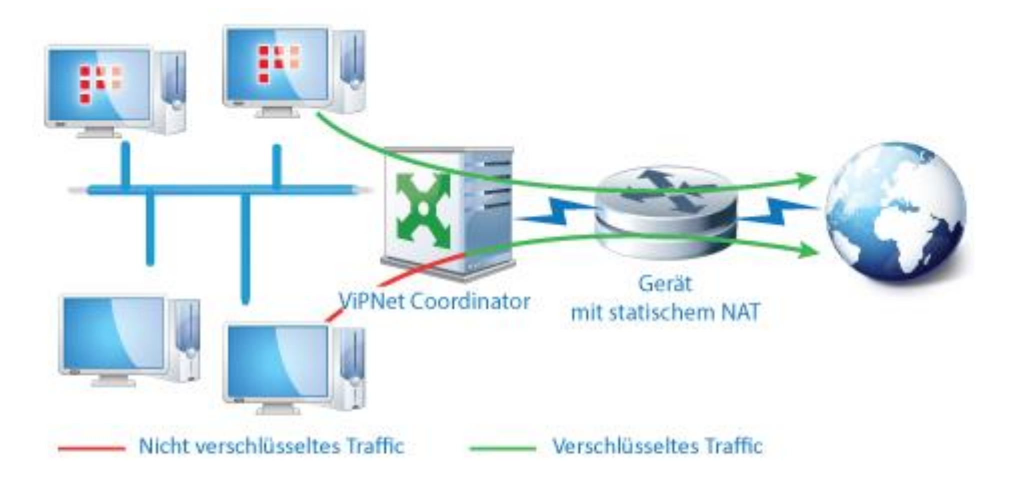


Abbildung 147. Verbindung des Coordinators über eine Firewall mit statischem NAT

Für ordnungsgemäße Verbindungen über eine Firewall mit statischem NAT sollte die IP-Adresse der verwendeten Firewall in den Betriebssystemeinstellungen des Netzwerkknotens als Standardgateway definiert werden. Auf der Firewall selbst sollten folgende statische Regeln der Adressumsetzung konfiguriert werden:

- ausgehende UDP-Pakete mit Adressen und Ports von Netzwerkknoten, die sich hinter der Firewall befinden, durchlassen.
- eingehende UDP-Pakete mit einem Zielport, der in den Einstellungen der Clients als Port der UDP-Kapselung definiert ist, durchlassen und umleiten;



Achtung! Wenn mehrere Netzwerkknoten ein und dieselbe Firewall mit statischer Adressumsetzung benutzen, sollte für jeden Netzwerkknoten eine eigene UDP-Kapselungsportnummer definiert werden. Falls ein und dieselbe Portnummer von mehreren Netzwerkknoten verwendet wird, können Konflikte auftreten.

Zum Einstellen der Verbindung des Coordinators über eine Firewall mit statischem NAT:

1. Wählen Sie im Programmfenster von ViPNet Monitor im Menü **Service** den Eintrag **Anwendungseinstellungen**.
2. Wählen Sie im Fenster **Einstellungen** in der Navigationsleiste den Bereich **Privates Netzwerk** aus.

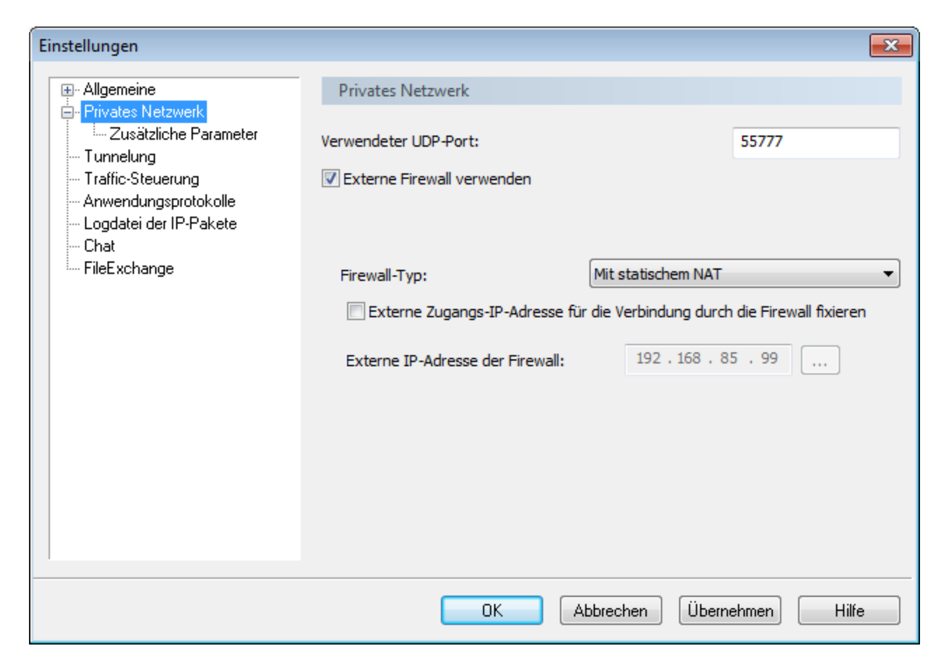


Abbildung 148. Verbindung des Coordinators über eine Firewall mit statischem NAT

3 Aktivieren Sie das Kontrollkästchen **Firewall verwenden** (in ViPNet Client) oder **Externe Firewall verwenden** (in ViPNet Coordinator).

4 Wenn Sie das Programm ViPNet Coordinator konfigurieren, wählen Sie in der Liste **IP-Adresse des Netzwerkadapters, der unmittelbar mit der Firewall verbunden ist** den Netzwerkadapter aus, über den die Verbindung zur Firewall erfolgen soll.

5 Wählen Sie die Option **Mit statischem NAT** in der Liste **Firewall-Typ** aus.

6 Ändern Sie bei Bedarf den Wert im Feld **Verwendeter UDP-Port**. Standardmäßig ist dort die Portnummer 55777 eingetragen. Die Portnummer sollte nur dann geändert werden, wenn mehrere Coordinatoren ein und dieselbe Firewall verwenden. In diesem Fall sollte jeder Coordinator über eine eigene Portnummer verfügen.

7 Wenn es notwendig ist, dass eingehende Pakete ungeachtet davon, von welcher Adresse die ausgehenden Pakete gesendet wurden, über eine bestimmte Adresse weitergeleitet, werden sollen, aktivieren Sie das Kontrollkästchen **Externe IP-Adresse für die Verbindung durch die Firewall fixieren** und wählen die benötigte IP-Adresse in der Liste **Externe IP-Adresse der Firewall** aus. Wählen Sie in der Liste **IP-Adresse des Netzwerkadapters, der unmittelbar mit der Firewall verbunden ist** den Netzwerkadapter aus, durch den die Verbindung zu der Firewall erfolgen soll.

   Diese Einstellung sollte nur dann verwendet werden, wenn die Firewall über mehrere externe IP-Adressen verfügt.

8 Klicken Sie auf die Schaltfläche **Übernehmen**, um die Einstellungen zu speichern.

Konfiguration der Netzwerkverbindung der Clients

Für die Verbindung des Clients mit dem privaten ViPNet Netzwerk sind im Regelfall keine Einstellungen nötig. Zusätzliche Einstellungen für die Verbindung können in einigen besonderen Fällen erforderlich sein. Beispiel: Sie verbinden sich über Ihren Laptop mit dem lokalen Netzwerk einer anderen Organisation, in der es keinen Zugang zu Ihrem Verbindungsserver gibt, wo aber ein eigener Coordinator zur Verfügung steht, der mit Ihrem Knoten verbunden ist. In diesem Fall sollten Sie den Verbindungsserver in den Verbindungseinstellungen für das ViPNet Netzwerk ändern.



Tipp. Wenn Sie sich häufig mit anderen lokalen Netzwerken verbinden, dann können Sie eine Konfiguration erstellen, in der Sie diese Variante der Verbindungseinstellungen speichern. Weitere Informationen über das Erstellen von Konfigurationen s. Abschnitt Steuerung von Programmkonfigurationen (auf S. 331).

Sie können einen anderen Verbindungsserver auch dann auswählen, wenn Ihr Coordinator aus irgendwelchen Gründen nicht erreichbar ist.

Führen Sie die folgenden Schritte aus, um einen Verbindungsserver festzulegen:

1 Wählen Sie im Programmfenster von ViPNet Monitor im Menü **Service** den Punkt **Anwendungseinstellungen**.

2 Wählen Sie im Fenster **Einstellungen** in der Navigationsleiste den Bereich **Privates Netzwerk**.

3 Wählen Sie in der Liste **Verbindungsserver** den Coordinator aus, mit dessen Hilfe der Client seine Verbindungen zu anderen Knoten herstellen soll. Wenn der erforderliche Coordinator nicht in der Liste enthalten ist, klicken Sie auf die Schaltfläche und wählen Sie den Coordinator im Fenster **Netzwerkknoten auswählen** aus.

4 Klicken Sie auf Übernehmen, um die Änderungen zu speichern.

Bei Bedarf können Sie die erweiterten Verbindungseinstellungen des Netzwerks konfigurieren:

- Klicken Sie auf Erweiterte Optionen Anzeigen im Fenster **Einstellungen** im Bereich **Privates Netzwerk** und führen Sie folgende Schritte aus:
  - Wenn der gesamte ein- und ausgehende Traffic über den Verbindungsserver geleitet werden soll, dann aktivieren Sie das Kontrollkästchen **Gesamten Traffic über den Verbindungsserver weiterleiten**.



Hinweis. Die Weiterleitung des IP-Traffics über einen Verbindungsserver kann dann erforderlich sein, wenn der gesamte übermittelte IP-Traffic überwacht werden soll. Dabei sollte beachtet werden, dass die Weiterleitung des IP-Traffics über den Verbindungsserver zu einer deutlichen Verringerung der Datenübertragungsgeschwindigkeit zwischen den Knoten führen kann.

- Wenn sich der Client über eine Firewall mit statischem NAT mit dem externen Netzwerk verbinden soll, dann aktivieren Sie das Kontrollkästchen **UDP-Port fixieren** und geben Sie den UDP-Kapselungsport im Eingabefeld darunter an.
- Wenn das Intervall für den Versand der IP-Pakete an den Verbindungsserver beim Arbeiten über eine Firewall mit dynamischem NAT geändert werden soll, dann geben Sie im Feld **Timeout für die Aufrechterhaltung von Verbindungen über Geräte mit dynamischem NAT** den neuen Wert an. Standardmäßig erfolgt der Versand der IP-Pakete alle 25 Sekunden. Im Regelfall genügt dieses Intervall, um eine Verbindung zum Verbindungsserver bei Verwendung der meisten NAT-Geräte aufrecht zu erhalten.
- Wenn Sie den IP-Adressenserver ändern sollen, wählen Sie einen anderen IP-Adressenserver in der Liste **IP-Adressenserver**.



Achtung! Es wird ausdrücklich davon abgeraten, den IP-Adressenserver ohne Rücksprache mit dem ViPNet Netzwerkadministrator zu ändern.

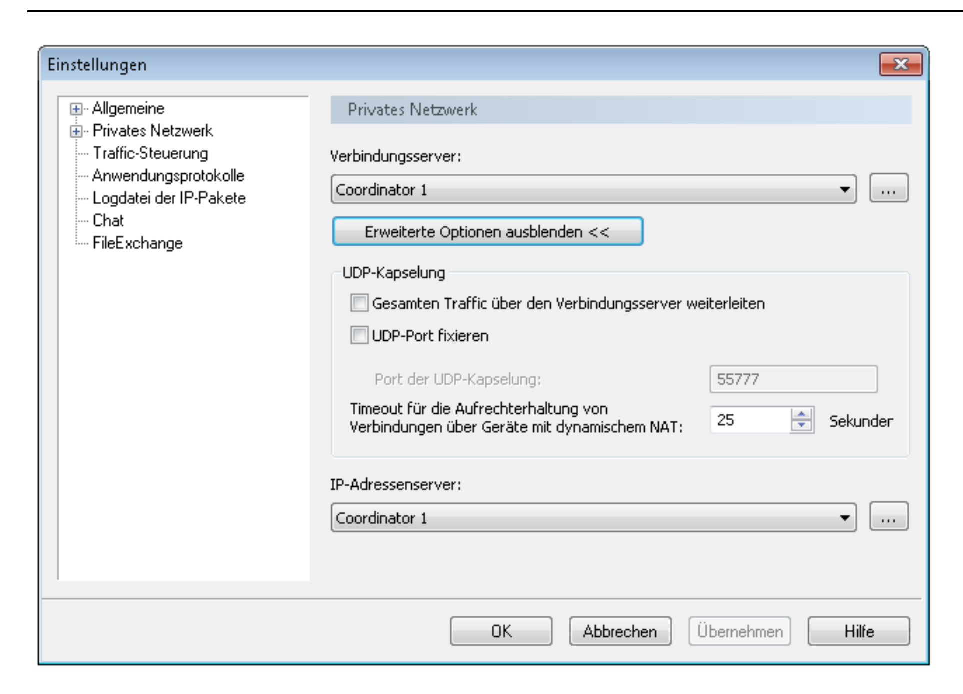


Abbildung 149. Verbindungsparameter des Clients

- Wenn es während der Arbeit mit bestimmten DSL-Modems Probleme bei der Übertragung großer Pakete gibt, dann gehen Sie zu den Bereich **Privates Netzwerk** > **Zusätzliche Parameter** und verringern den Wert des Parameters MSS (Maximum Segment Size).

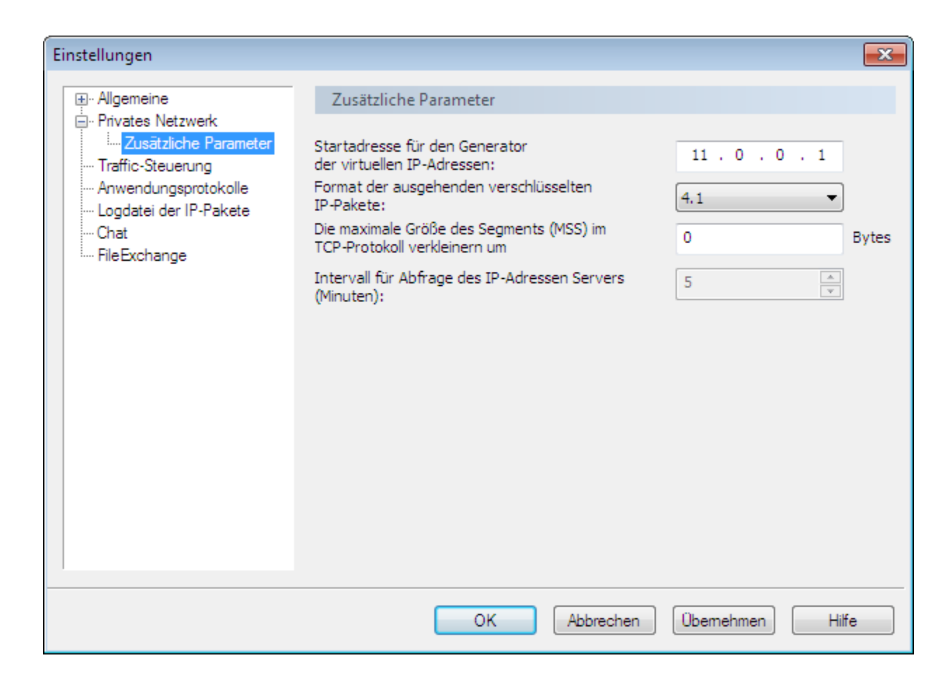


Abbildung 150. Einstellung zusätzlicher Parameter

Klicken Sie zum Speichern der Parameter der erweiterten Einstellungen auf die Schaltfläche **Übernehmen**.

Verwenden von virtuellen IP-Adressen

In den unterschiedlichen lokalen Netzwerken und in den Netzwerken der Internetanbieter tritt häufig das Problem der Überschneidung von IP-Adressen auf. Die Technologie der virtuellen Adressen ermöglicht es, dieses Problem beim Einrichten von geschützten Verbindungen effektiv zu lösen.

Virtuelle Adressen können auch dazu verwendet werden, den Zugang zu bestimmten Objekten anhand der virtuellen Adressen zu regeln. Wozu ist es nützlich? Bekanntermaßen kann eine IP-Adresse zur Benutzer-Identifizierung verwendet werden, d. h. eine Fälschung der IP-Adresse stellt eine bedeutende Gefahr für das Netzwerk dar. In einem ViPNet Netzwerk ist das Fälschen von IP-Adressen jedoch nicht möglich. Beim Empfang eines Pakets aus dem Netzwerk ersetzt der ViPNet Treiber die reelle IP-Adresse des Absenders durch eine entsprechende virtuelle Adresse und leitet das Paket anschließend weiter. Dies passiert jedoch nur nach einer erfolgreichen Entschlüsselung des Pakets anhand der Absenderschlüssel, d. h. nachdem der Paketabsender identifiziert wurde. Diese Vorgangsweise schützt das System vor einer Fälschung der Absenderadresse und gewährleistet die Abgrenzung des Zugriffs auf Netzwerkressourcen mit Hilfe von virtuellen Adressen.

Jeder ViPNet Netzwerkknoten bildet automatisch eine oder mehrere virtuelle IP-Adressen für jeden ViPNet Netzwerkknoten und für jeden getunnelten Knoten, mit dem er verbunden ist. Jeder reellen Adresse des Knotens wird eine virtuelle IP-Adresse gegenübergestellt. D. h., die Anzahl der gebildeten virtuellen Adressen hängt von der Anzahl der reellen Adressen des Knotens und der Anzahl der von diesem Knoten getunnelten Adressen ab.

Jeder Netzwerkknoten verfügt über eine eigene Liste von virtuellen Adressen für die anderen Knoten. Alle Anwendungen können diese virtuellen Adressen bei ihrer Arbeit im Netzwerk für die Verbindungen mit den entsprechenden Knoten verwenden. Der ViPNet Treiber ersetzt die Adressen zum Sende- und Empfangszeitpunkt der IP-Pakete (einschließlich der Pakete der DNS-, WINS-, NetBIOS-, SCCP-, SIP- und anderer Dienste).

Standardmäßig verwendet ein Netzwerkknoten die virtuellen Adressen für die Verbindungen mit den anderen Netzwerkknoten, falls diese Netzwerkknoten über die Broadcast-IP-Adressen nicht zugänglich sind. Für getunnelte Knoten werden normalerweise reelle IP-Adressen verwendet. Bei Bedarf kann für jeden beliebigen Knoten zwangsweise seine reelle oder virtuelle Sichtbarkeit eingestellt werden.

Konfiguration des Zugangs zu geschützten Netzwerkknoten

Wenn im ViPNet Netzwerk mehrere Coordinatoren eingerichtet sind, sollten zuallererst Verbindungen zwischen diesen Coordinatoren hergestellt werden. Dies ist nötig, damit die Coordinatoren Informationen über Zugangsparameter für Clients austauschen können, für die sie als IP-Adressenserver (auf S. 239) fungieren.

Zum Herstellen einer Verbindung zwischen zwei Coordinatoren sollte auf jedem Coordinator die IP-Adresse oder der DNS-Name des Coordinators angegeben werden, zu dem die Verbindung eingerichtet werden soll.

Die Clients erhalten alle erforderlichen Zugangsparameter für den Zugriff auf andere Netzwerkknoten automatisch von ihrem IP-Adressenserver.



Hinweis. Wenn IP-Adressen und Verbindungsparameter der Coordinatoren im Programm ViPNet Network Manager früher eingestellt wurden, sind keine zusätzliche Einstellungen im Programm ViPNet Monitor erforderlich.

Gehen Sie wie folgt vor, um die Zugangsparameter zu einem geschützten ViPNet Netzwerkknoten einzustellen:

1 Wählen Sie im Programmfenster von ViPNet Monitor in der Navigationsleiste den Bereich **Privates Netzwerk** aus.

2 Doppelklicken Sie im Bereich **Privates Netzwerk** auf den benötigten Netzwerkknoten.

3 Fügen Sie im Fenster **Netzwerkknoten-Eigenschaften** in der Registerkarte **IP-Adressen** die reelle IP-Adresse des Netzwerkknotens in der Liste hinzu. Der neuen Adresse wird automatisch eine virtuelle IP-Adresse zugeordnet.

   Wenn Sie die IP-Adresse des Knotens nicht kennen, können Sie die Adresse anhand des Computernamens ermitteln. Klicken Sie dazu auf die Schaltfläche **Name/IP-Adresse auflösen** und führen im eingeblendeten Fenster die Suche nach der benötigten IP-Adresse anhand des Computernamens durch.

   Beim Hinzufügen einer IP-Adresse wird automatisch überprüft, ob es Konflikte mit IP-Adressen gibt, die bereits in der Liste enthalten sind. Außerdem wird überprüft, ob die neue Adresse im Konflikt mit den IP-Adressen anderer Netzwerkknoten (inklusive getunnelter Knoten) steht, falls für diese Knoten keine Sichtbarkeit der virtuellen IP-Adressen festgelegt wurde. Diese Überprüfung dient dazu, das Hinzufügen von identischen IP-Adressen zu vermeiden. Wenn im Zuge der Überprüfung sich überschneidende Einträge festgestellt werden, wird eine entsprechende Fehlermeldung angezeigt. Beheben Sie den IP-Adressenkonflikt.

   Sie können die Überprüfung auf eine mögliche Überschneidung der IP-Adressen auch manuell durchführen. Klicken Sie dazu auf die Schaltfläche **Konflikte überprüfen** .

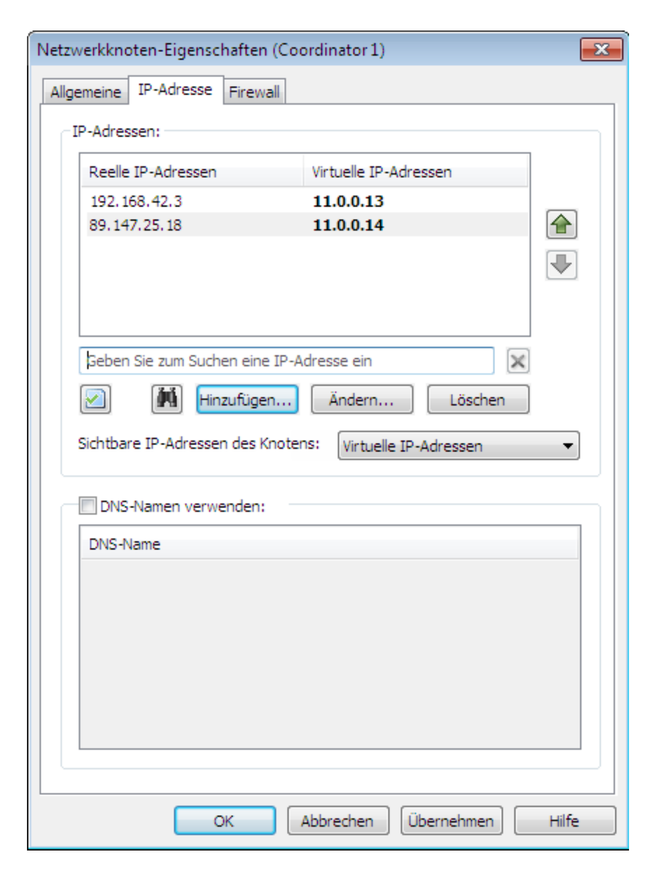


Abbildung 151. IP-Adressen eines Netzwerkknotens

4 Geben Sie in der Liste **Sichtbare IP-Adressen des Knotens** an, über welche Adressen der betroffene Netzwerkknoten erreichbar sein soll. Standardmäßig werden die sichtbare IP-Adressen der Knoten automatisch festgelegt. Wenn Konflikte reeller IP-Adressen mit den Adressen anderer Knoten im Netzwerk möglich sind, dann wählen Sie den Eintrag **Virtuelle IP-Adressen**.

Bei einer Änderung der sichtbaren IP-Adressen in den Coordinator-Eigenschaften schlägt das System vor, die gleiche sichtbare IP-Adressen für alle Knoten festzulegen, die den gegebenen Coordinator als Verbindungsserver verwenden.

5 Wenn für den Zugang zum Netzwerkknoten die Verwendung seines DNS-Namens notwendig ist, aktivieren Sie das Kontrollkästchen **DNS-Name verwenden** und fügen den DNS-Namen des Netzwerkknotens in der Liste hinzu. Beim Hinzufügen eines DNS-Namens wird der Name auch automatisch geprüft, ob er mit den im Programm bereits angegebenen DNS-Namen in Konflikt steht. Stellt sich im Zuge der Überprüfung ein Konflikt zwischen DNS-Namen heraus, lösen Sie den Konflikt. Sie können auch überprüfen, ob es einen Konflikt zwischen DNS-Namen gibt, indem Sie auf die Schaltfläche **Konflikte überprüfen** klicken

Jedem Netzwerkknoten können mehrere DNS-Namen zugewiesen werden. Bei der Einstellung der Zugangsparameter zu einem Coordinator sollten die DNS-Namen der durch diesen Coordinator getunnelten Knoten ebenfalls zur Liste in der Registerkarte **IP-Adresse** hinzugefügt werden.

Bei einem Client spielt die Reihenfolge der DNS-Namen in der Liste keine Rolle. Bei einem Coordinator sollte an der ersten Stelle der DNS-Name stehen, der der IP-Adresse des Coordinators entspricht. Weitere Informationen zur Verwendung des DNS-Dienstes in ViPNet Netzwerken finden Sie im Kapitel Konfiguration und Verwendung der Namensdienste DNS und WINS im ViPNet Netzwerk (auf S. 305).

6 Fügen Sie bei der Konfiguration der Zugangsparameter für den Coordinator in der Registerkarte **Firewall** die IP-Adresse der Firewall hinzu (falls eine Firewall verwendet wird). Geben Sie bei Bedarf zusätzliche IP-Adressen an. Wenn mehrere IP-Adressen für den Zugang über eine Firewall angegeben werden, dann können Sie die Prioritäten dieser Adressen mit Hilfe von Metriken festlegen.

Geben Sie im Feld UDP-Port den Port des Zugangs über die Firewall an.

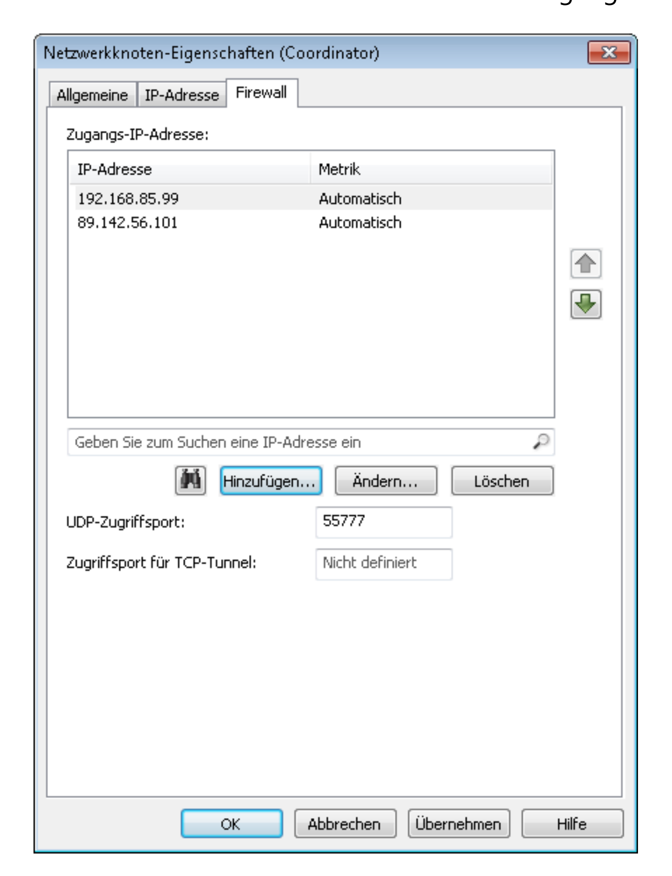


Abbildung 152. Einstellung des Zugangs zu einem Netzwerkknoten über eine Firewall

7 Bei der Konfiguration der Zugangsparameter des Coordinators können Sie auf der Registerkarte **Firewall** im Feld **Zugriffsport für TCP-Tunnel** den Port angeben, der von Ihrem Knoten für die Verbindung zum Coordinator über das TCP-Protokoll (TCP-Tunnel) verwendet wird. Es wird empfohlen, diesen Port dann anzugeben, wenn er nicht bereits in den Coordinator-Eigenschaften definiert wurde und wenn gleichzeitig bekannt ist, dass auf dem gegebenen Coordinator ein TCP-Tunnel für Verbindungen über das TCP-Protokoll eingerichtet ist.

Im Regelfall werden die Informationen über die Portnummer für den Zugang über das TCP-Protokoll sofort nach der Konfiguration des TCP-Tunnels auf dem Coordinator an den Netzwerkknoten weitergeleitet. Wenn also der Zugangsport für die Verbindungen über das TCP-Protokoll in den Eigenschaften des Coordinators definiert ist, sollte der eingetragene Wert nicht geändert werden.

8 Klicken Sie auf die Schaltfläche **Übernehmen**, um die Einstellungen zu speichern.

Konfiguration des Zugangs zu getunnelten Netzwerkobjekten

Falls Coordinator eine Funktion der Tunnelung offener Netzwerkknoten durchführt, sollen entsprechende Einstellungen für diesen Coordinator im Programm ViPNet Network Manager (s. Tunnelung auf S. 114) oder ViPNet Coordinator Monitor (s. Schutz des Traffics offener Netzwerkknoten (Tunnelung) auf S. 299) angegeben werden.

Falls ein Client muss Verbindungen mit getunnelten Knoten erstellen (oder ein Coordinator muss Verbindungen mit anderen Knoten, die durch anderen Coordinator getunnelt werden, erstellen), sollen im Programm ViPNet Monitor auf diesem Knoten Parameter des Zugangs zu getunnelten Knoten eingestellt werden. Diese Parameter werden für die Clients standardmäßig im Administratormodus konfiguriert.

Wenn die Tunnelungsparameter für sämtliche Coordinatoren bereits im Programm ViPNet Network Manager konfiguriert wurden, dann sind im Programm ViPNet Monitor auf dem Netzwerkknoten keine weiteren Einstellungen mehr nötig. Der Netzwerkknoten wird in der Lage sein, Verbindungen zu getunnelten Knoten aufzubauen. Wenn diese Einstellungen nicht im Voraus vorgenommen wurden, dann sollten Sie die Parameter der Verbindung zu getunnelten Knoten auf Ihrem Netzwerkknoten manuell einstellen. Führen Sie dazu die folgenden Schritte aus:

1 Wählen Sie im Programmfenster von ViPNet Monitor in der Navigationsleiste den Bereich **Privates Netzwerk** aus.

2 Doppelklicken Sie im Bereich **Privates Netzwerk** auf den Coordinator, der die Tunnelung des gegebenen offenen Netzwerkknotens durchführt.

3 Aktivieren Sie im Fenster **Netzwerkknoten-Eigenschaften** in der Registerkarte **Tunnel** das Kontrollkästchen **IP-Adressen, die getunnelt werden** und erstellen mit Hilfe der entsprechenden Schaltflächen eine Liste der IP-Adressen der getunnelten Knoten. Den angegebenen IP-Adressen werden automatisch virtuelle IP-Adressen zugeordnet.

   Wenn Ihnen die IP-Adresse des getunnelten Knotens nicht bekannt ist, können Sie die Adresse anhand des Computernamens ermitteln. Klicken Sie dazu auf die Schaltfläche **Name/IP-Adresse auflösen** und führen im eingeblendeten Fenster eine Suche nach der IP-Adresse anhand des Computernamens durch.



Hinweis. Wenn die DNS-Namen der getunnelten Objekte verwendet werden sollen, dann fügen Sie diese Namen in der Liste der DNS-Namen auf dem tunnelnden Coordinator hinzu. Beachten Sie, dass an der ersten Stelle dieser Liste der auf dem DNS-Server registrierte Name des Coordinators stehen muss.

Beim Hinzufügen der IP-Adresse wird automatisch überprüft, ob sich die angegebene Adresse mit den Adressen in der Liste oder mit den IP-Adressen anderer Netzwerkknoten (inklusive getunnelter Knoten) überschneidet. Diese Überprüfung dient dazu, das Hinzufügen von identischen IP-Adressen

zu vermeiden. Wenn im Zuge der Überprüfung sich überschneidende Einträge festgestellt werden, wird eine entsprechende Fehlermeldung angezeigt. Beheben Sie die Überschneidung der IP-Adressen.

Sie können die Überprüfung auf eine mögliche Überschneidung der IP-Adressen auch manuell durchführen. Klicken Sie dazu auf die Schaltfläche **Konflikte überprüfen** .

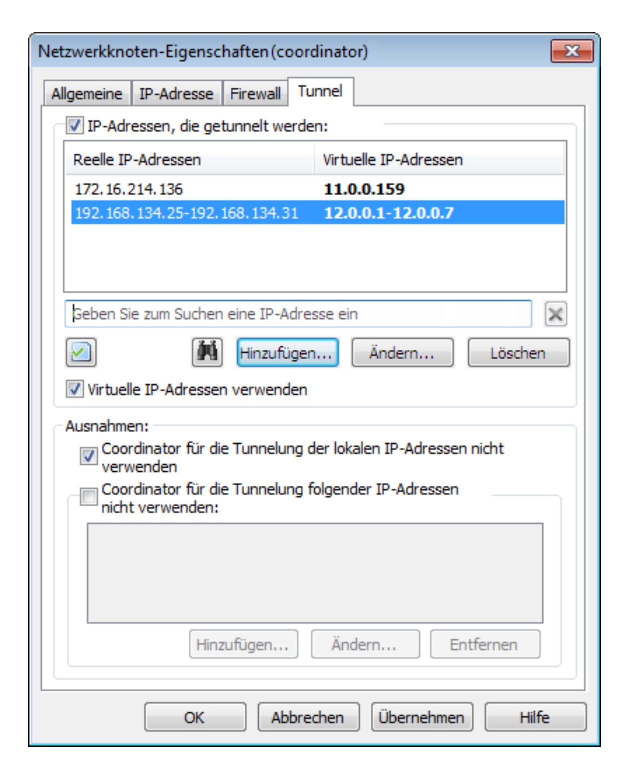


Abbildung 153. Adressen der getunnelten Netzwerkknoten

4 Aktivieren Sie das Kontrollkästchen **Virtuelle IP-Adressen verwenden**, wenn Konflikte zwischen den IP-Adressen der Subnetze möglich sind.

5 Wenn sich der getunnelte Knoten im gleichen Subnetz wie Ihr eigener Knoten befindet und wenn dort kein Sonderrouting eingestellt ist, dann stellen Sie sicher, dass das Kontrollkästchen **Coordinator für die Tunnelung der lokalen IP-Adressen nicht verwenden** aktiviert ist. Anderenfalls wird eine Verbindung mit dem getunnelten Knoten nicht möglich sein.

6 Falls der Traffic bei Verbindungen zu irgendwelchen getunnelten Netzwerkknoten nicht verschlüsselt werden soll, dann ist es empfehlenswert, das Kontrollkästchen **Coordinator für die Tunnelung folgender IP-Adressen nicht verwenden** zu aktivieren und die IP-Adressen der betroffenen Netzwerkknotens in die Liste darunter einzutragen

7 Nachdem alle Einstellungen vorgenommen wurden, klicken Sie auf die Schaltfläche **Übernehmen**.

Die in diesem Kapitel beschriebenen Einstellungen müssen auf dem Netzwerkknoten für alle Coordinatoren vorgenommen werden, deren getunnelte Netzwerkobjekte, vom Knoten erreicht werden sollen.

Konfiguration des TCP-Tunnels

Bei Remoteverbindungen der Clients zu ViPNet Netzwerken können manchmal Probleme bei der Übermittlung der IP-Pakete über das UDP-Protokoll auftreten, da dieses Protokoll von einigen Serviceanbietern blockiert wird. Für die Kommunikation der ViPNet Netzwerkknoten können Verbindungen über einen TCP-Tunnel unter Verwendung des TCP-Protokolls eingerichtet werden, um dieses Problem zu lösen. Dazu sollte auf dem Verbindungsserver, über welchen die Weiterleitung der IP-Pakete erfolgt, ein TCP-Tunnel konfiguriert werden (s. TCP-Tunnel auf S. 244).



Hinweis. Ein TCP-Tunnel kann nur auf einem Coordinator eingerichtet werden, auf dem das Kontrollkästchen **Externe Firewall verwenden** deaktiviert ist oder Firewall-Typ **Mit statischem NAT** ausgewählt ist.

Führen Sie die folgenden Schritte aus, um einen TCP-Tunnel auf dem Coordinator zu konfigurieren:

1 Wählen Sie im Programmfenster von ViPNet Monitor im Menü **Service** den Punkt **Anwendungseinstellungen**.

2 Wählen Sie im Fenster **Einstellungen** in der Navigationsleiste den Bereich **Privates Netzwerk**.

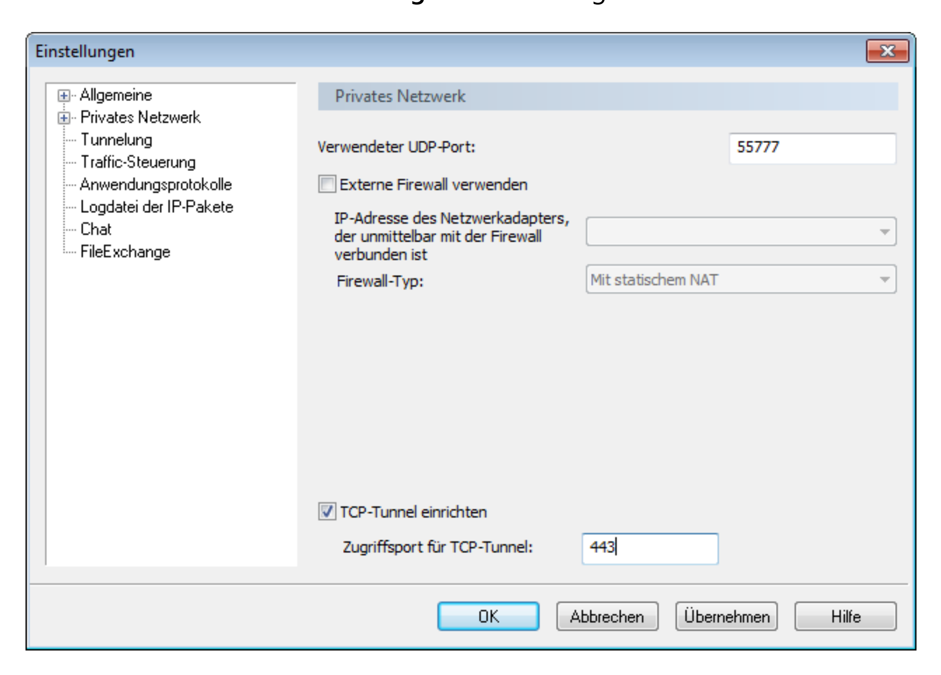


Abbildung 154. Konfiguration des TCP-Tunnels

3 Aktivieren Sie das Kontrollkästchen **TCP-Tunnel einrichten**.

4 Geben Sie im Feld **Zugriffsport für TCP-Tunnel** die Nummer des Ports an, auf welchem die TCP-Pakete der geschützten Knoten eintreffen werden.

5 Klicken Sie zum Speichern der Einstellungen auf die Schaltfläche **Übernehmen**.

Dadurch wird ein TCP-Tunnel auf dem Coordinator eingerichtet. Die Informationen über den neuen TCP-Tunnel mitsamt der Portnummer für die Weiterleitung der TCP-Pakete werden an alle Netzwerkknoten versendet, für welche der gegebene Coordinator als Verbindungsserver auftritt.

Wenn ein Remoteclient im Weiteren nicht in der Lage ist, eine Verbindung zu den anderen ViPNet Netzwerkknoten über das UDP-Protokoll herzustellen, dann beginnt dieser Client automatisch, die benötigten Verbindungen über den TCP-Tunnel aufzubauen, der auf seinem Verbindungsserver konfiguriert ist. Die erhaltenen IP-Pakete werden auf dem Coordinator aus dem TCP-Tunnel extrahiert und dann über das UDP-Protokoll an die Zielknoten weitergeleitet.

12

Integrierte Firewall

Einsatz der integrierten Firewall

Auf den geschützten ViPNet Netzwerkknoten kann man außerdem die in den Programmen ViPNet Client und ViPNet Coordinator integrierten Firewalls verwenden. Das Programm ViPNet Client stellt die Funktionen einer für jedes Benutzerkonto separat konfigurierbaren Firewall. Das Programm ViPNet Coordinator agiert selbst als eine Firewall, indem es offene lokale und Transitverbindungen anhand von bestimmten Regeln filtert, sowie die Übersetzung der IP-Adressen (die NAT-Funktion) für das durchgehende Traffic übernimmt.

Standardmäßig verfügen die Clients und Coordinatoren eines ViPNet Netzwerks über voreingestellte Netzwerkfilter, die den gesamten offenen Traffic durchlassen, d.h. die integrierte ViPNet VPN Firewall ist deaktiviert. Das beugt Konfliktsituationen und Internetzugangsstörungen vor, im Fall wenn auf dem Knoten eine andere Firewall aktiviert ist (z.B. Windows Firewall).

Außerdem können Sie mit Hilfe der ViPNet VPN Software die für das offene Netzwerk erstellten Filter zentralisiert auf die geschützten Netzwerkknoten anwenden. Dafür wird das Programm ViPNet Policy Manager eingesetzt, mit dessen Hilfe Sie Netzwerkfilter und NAT-Regeln erstellen und danach als Teil einer Sicherheitsrichtlinie an Knoten Ihres ViPNet VPN Netzwerkes übertragen können. Die vom ViPNet Policy Manager abgeschickten Filter und Regeln werden auf den Clients und Coordinatoren des Netzwerks automatisch angewendet. Sie sind nicht editierbar, haben einer höhere Priorität und werden deswegen als Erstes ausgeführt. Wir empfehlen Ihnen die Sicherheitsrichtlinien im Programm ViPNet Policy Manager zu verwalten (detaillierte Anleitung dafür finden Sie im Dokument „ViPNet Policy Manager. Administratorhandbuch“). Sollte das Programm ViPNet Policy Manager nicht im Einsatz sein, können Sie Ihre eigenen Netzwerkfilter in den Programmen ViPNet Client und ViPNet Coordinator erstellen.

Folgende Möglichkeiten stehen Ihnen bei der Verwendung der integrierten ViPNet VPN Firewall zur Verfügung:

1. Den unerwünschten Traffic blockieren (wird empfohlen). Führen Sie hierfür folgende Aktionen durch:
   - Erstellen Sie Ihre eigenen Filter, die den unerwünschten Traffic blockieren.
   - Setzen Sie die integrierte ViPNet VPN Firewall parallel zu anderen Firewalls ein.
2. Den gesamten offenen Traffic blockieren und nur bestimmten Traffic erlauben.



Achtung! Diese Methode sollte nur von erfahrenen Administratoren verwendet werden.

Dafür machen Sie folgendes:

- Löschen Sie den Standardfilter, der den gesamten offenen Traffic erlaubt. Der Filter, welcher den gesamten Traffic blockiert, wurde bereits bei der Programminstallation automatisch angelegt und ist nicht editierbar.
- Erstellen Sie Ihre eigenen Filter, die den notwendigen Traffic erlauben und deaktivieren alle anderen Firewalls (einschließlich der Windows Firewall).

Grundprinzipien der Traffic-Filterung

Gefiltert wird der gesamte Traffic, der einen Netzwerkknoten durchläuft:

- offener (nicht verschlüsselter) Traffic;
- geschützter (verschlüsselter) Traffic;
- getunnelter Traffic.

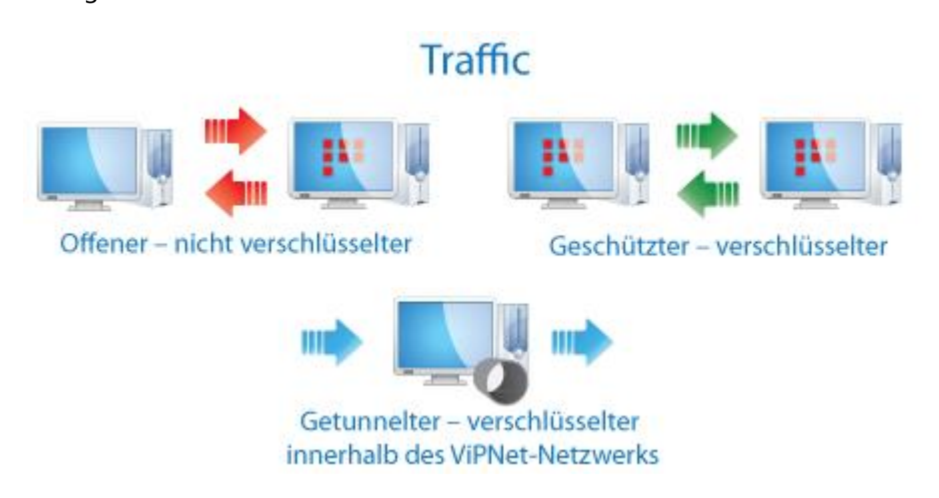


Abbildung 155. IP-Traffic-Typen

Die größte Gefahr stellt der Traffic aus offenen Netzwerken dar, da die Gefahrenquelle im Fall von Angriffen nur schwer festgestellt und entsprechende Gegenmaßnahmen nicht sofort gesetzt werden können.

Sowohl beim offenen als auch beim verschlüsselten Traffic kann es sich um lokalen oder Broadcast-Traffic handeln. Als lokaler Traffic wird der gesamte ein- oder ausgehende Traffic eines bestimmten Knotens bezeichnet (d. h. der Netzwerkknoten tritt als Absender oder Empfänger der IP-Pakete auf). Als Broadcast-Traffic wird die Weiterleitung von IP-Paketen durch einen Knoten bezeichnet, wobei die IP- oder MAC-Zieladresse des Pakets eine Broadcast-Adresse darstellt (d. h. die Pakete werden an alle Knoten eines bestimmten Netzwerksegments adressiert).

Zusätzlich kann es sich um Transit-Traffic auf dem Coordinator handeln. Als Transit-Traffic wird der Traffic bezeichnet, bei dem der Coordinator weder als Absender noch als Empfänger auftritt (d. h. der Traffic wird über den Coordinator lediglich weitergeleitet).

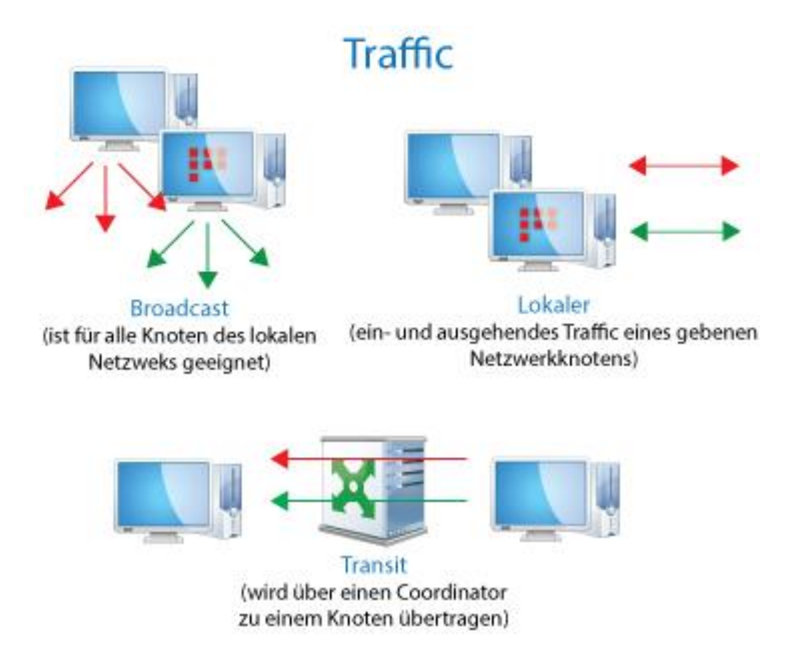


Abbildung 156. Typen von geschützten und offenen Traffic

Um die Filterregeln richtig einzustellen, wird das Verständnis grundsätzlicher Filterungsprinzipien unterschiedlicher Traffic-Typen benötigt.

Alle ein- und ausgehenden, offenen und verschlüsselten IP-Pakete werden einer komplexen Filterung in folgender Reihenfolge unterzogen:

1 Überprüfung in Übereinstimmung mit den Antispoofing-Regeln.



Hinweis. Diese Überprüfung wird nur bei der Filterung des offenen Traffics einschließlich des Traffics zwischen dem Coordinator und den von ihm getunnelten Geräten durchgeführt.

Wenn die IP-Paketsadresse der Antispoofing-Regel entspricht, wird diese IP-Pakete erlaubt. Anderenfalls wird das Paket blockiert.

2 Überprüfung in Übereinstimmung mit den Netzwerkfiltern, die vom Benutzer konfiguriert wurden. Wenn die Parameter des IP-Pakets mit den Parametern eines der konfigurierten Filter übereinstimmen, dann wird das Paket gemäß den Filtereinstellungen durchgelassen oder blockiert. Wenn das IP-Paket keinem einzigen der konfigurierten Filter entspricht, dann wird es blockiert.

Die Reihenfolge der Filterung der IP-Pakete wird in der folgenden Abbildung schematisch dargestellt:

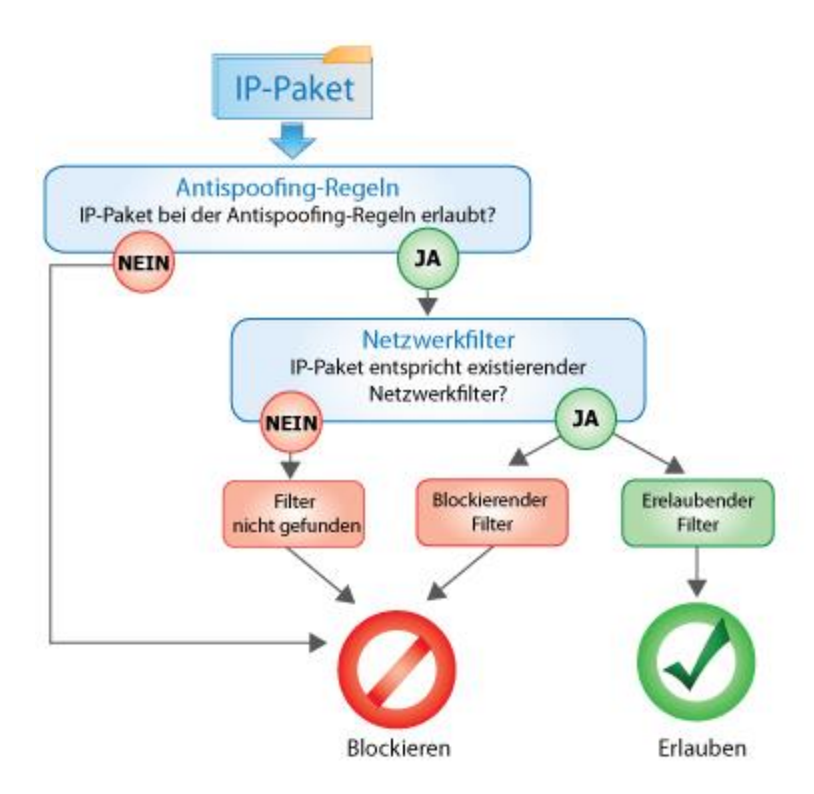


Abbildung 157. Filterungsstufen des offenen Datenverkehrs

Diese Art der Filterung gewährleistet ein hohes Ausmaß an Sicherheit, da Verbindungen ausschließlich zu benötigten Knoten und über vordefinierte Protokolle und Ports erlaubt werden. Das IP-Paket wird konsequent von einer Reihe von Filtern überprüft, bis es entweder durchgelassen oder von einem der Filter blockiert wird. Wenn das Paket von keinem einzigen Filter verarbeitet wurde, dann wird es blockiert.

Auf verschlüsselte IP-Pakete werden die Netzwerkfilter nur dann angewendet, wenn das Paket erfolgreich entschlüsselt und der Quell-Knoten des Pakets innerhalb des Netzwerks identifiziert wurde. In diesem Fall sind die IP-Adressen der Netzwerkknoten nicht von Bedeutung.



Hinweis. Im Software ViPNet Monitor Version 3.2 und niedriger wurde der Traffic-Filterungsprinzip von dem ausgewählten Sicherheitsstufe bestimmt.

Allgemeine Informationen über Netzwerkfilter

Die Netzwerkfilter werden für den verschlüsselten, offenen und den getunnelten Traffic separat definiert. Sie erfüllen die folgenden Funktionen:

- Die lokale Filter des offenen Netzwerks auf dem Netzwerkknoten können den IP-Datenaustausch mit offenen Knoten erlauben oder blockieren.



Hinweis. Als offen werden Knoten bezeichnet, auf denen keine ViPNet Software mit Traffic-Verschlüsselungsfunktion installiert ist.

Für die Netzwerkclients sind standardmäßig beliebige Verbindungen zu den offenen Knoten erlaubt. Bei Bedarf können Sie andere Filter des offenen Netzwerks für diese Clients einstellen oder entsprechende Einstellungen für die Firewalls der Drittanbieter vornehmen (falls solche Firewalls auf den Clients installiert sind).

- Die Filter des privaten Netzwerks können den IP-Datenaustausch mit geschützten ViPNet Knoten, zu denen der gegebene Knoten Verbindungen aufbauen kann, begrenzen.
- Die Filter für den getunnelten Traffic legen Regeln für IP-Pakete fest, die zwischen getunnelten Knoten und ViPNet Netzwerkknoten, mit denen der betroffene Coordinator verbunden ist, übermittelt werden.

Netzwerkfilter werden unabhängig von ihrer funktionellen Bestimmung in drei Kategorien unterteilt:

- Filter, die als Inhalt von Sicherheitsrichtlinien aus dem Programm ViPNet Policy Manager versendet wurden.

  Mit Hilfe einer Sonderoption können diese Filter im Administrator-Modus aus den Listen der Netzwerkfilter ausgeschlossen werden.

- Vorinstallierte und benutzerdefinierte Filter.

  Falls das Programm ViPNet Monitor von Version 3.x auf die Version 4.x aktualisiert wurde, sind keine vorinstallierten Filter im Programm vorhanden. In den Listen der Netzwerkfilter sind lediglich Filter enthalten, die vor dem Update erstellt wurden (in konvertierter Form).

- Standardmäßig konfigurierte Filter.

Die vom ViPNet Policy Manager verteilten Filter werden nach seiner Priorität als wichtiger angesehen als alle anderen Filter und können nicht geändert werden. Diese Filter können nicht geändert werden. Nach ihnen folgen vorinstallierte Filter und Filter, die vom Benutzer im Programm ViPNet Monitor erstellt wurden. Bei Vorliegen bestimmter Berechtigungen können diese Filter jederzeit geändert oder gelöscht werden. Am Ende folgen die Standardfilter. Diese Kategorie der Filter umfasst nur einen Netzwerkfilter, der sämtlichen IP-Traffic blockiert, der von keinem der Netzwerkfilter der oberen Kategorien verarbeitet wurde.

Die Reihenfolge der Anwendung der Netzwerkfilter gemäß ihrer Priorität wird in der Abbildung unten dargestellt.

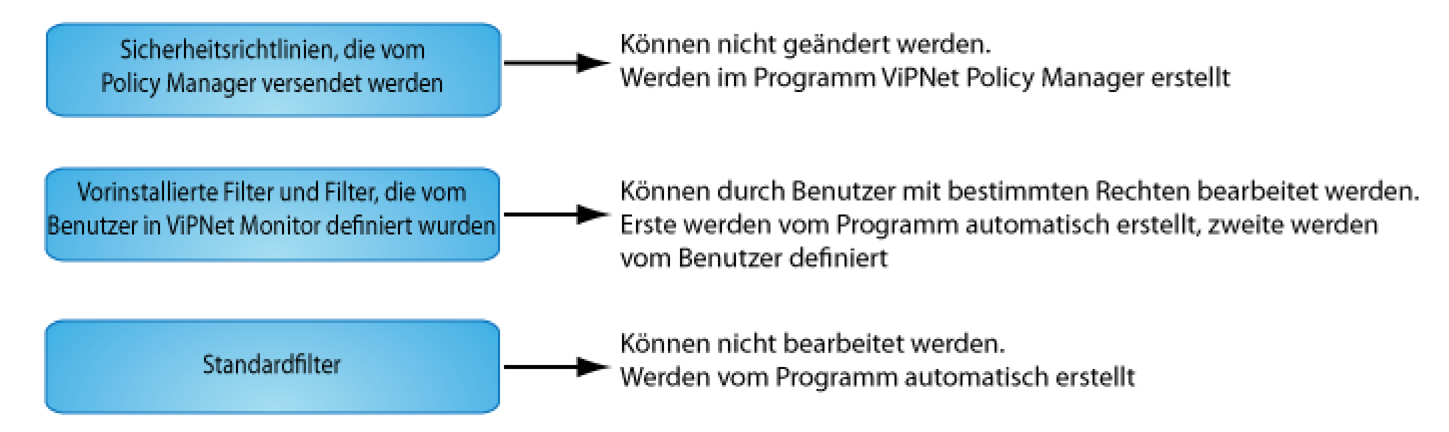


Abbildung 158. Priorität der Anwendung der Netzwerkfilter

Die Listen der Netzwerkfilter werden in der Panel-Ansicht in den folgenden Bereichen angezeigt:

- In ViPNet Client Monitor: **Filter des privaten Netzwerks**, **Offenes Netzwerk**.
- In ViPNet Coordinator Monitor: **Filter des privaten Netzwerks**, **Filter für getunnelte Knoten**, **Transit-Filter des offenen Netzwerks** und **Lokale Filter des offenen Netzwerks**.

Hinweis. In den Programmen ViPNet Client und ViPNet Coordinator sind standardmäßig Filter konfiguriert, die den gesamten Traffic sowohl des geschützten als auch des offenen Netzwerks durchlassen. Wenn eigene Filter definiert werden sollen, dann deaktivieren Sie zunächst die Windows-Firewall, um mögliche Konflikte zwischen dieser Firewall und den Programmen ViPNet Client und ViPNet Coordinator zu vermeiden

---

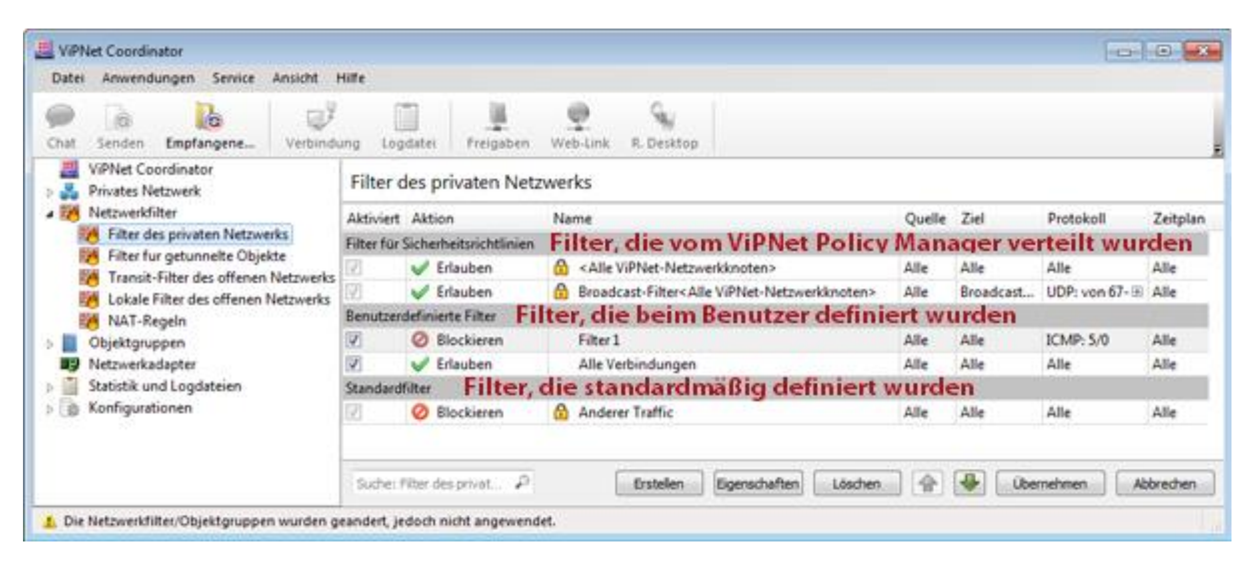


Abbildung 159. Beispiel für Anzeige von Filtern für den verschlüsselten Traffic unterschiedlicher Kategorien

Die Netzwerkfilter verfügen über folgende Besonderheiten:

- Ein Filter beinhalten die folgenden Parameter:

- Aktion, die auf betroffene IP-Pakete angewendet wird. IP-Pakete, die den vorgegebenen Parametern entsprechen, können vom Filter entweder erlaubt (✓) oder blockiert (✗) werden;
- Quelle und Ziel der IP-Pakete, die vom Filter erfasst werden;
- Protokolle der gefilterten IP-Pakete;
- Zeitpläne.

Zum Einstellen der Filterparameter können Objektgruppen verwendet werden.

- Benutzerdefinierte Filter haben Auswirkungen sowohl auf neue als auch auf bestehende Verbindungen. Wenn also ein blockierender Filter zu einem Zeitpunkt erstellt wird, zu dem bereits aktive Verbindungen bestehen, dann werden diese Verbindungen nach dem Aktivieren des Filters sofort unterbrochen.
- Die IP-Pakete werden in Übereinstimmung mit der Position der Filter in der Liste von oben nach unten abgearbeitet. Wenn ein Paket vom ersten passenden Filter blockiert oder erlaubt wird, dann sind alle nachfolgenden Filter für das gegebene Paket nicht mehr wirksam.
- Im Programm ViPNet Monitor werden die Filter unterschiedlicher Kategorien in der Liste von Filtern in verschiedenen Gruppen angezeigt und werden in der Reihenfolge ihrer Priorität in Übereinstimmung mit dem oben abgebildeten Schema angeordnet.

  Reihenfolge der Standardfilter und Filter, die vom ViPNet Policy Manager versendet wurden, kann nicht geändert werden. Die Reihenfolge der vorinstallierten Filter und der im Programm ViPNet Monitor definierten Filter können Sie mit Hilfe der Schaltflächen und ändern.
- Filter, die nicht geändert oder gelöscht werden können, werden durch das Symbol gekennzeichnet.
- Wenn Sie die Aktion eines Filtern ändern möchten, öffnen Sie per Doppelklick die Filter-Eigenschaften und wählen Sie im Bereich **Allgemeine Optionen** den benötigten Wert. Zum (De-)Aktivieren eines Filters aktivieren oder deaktivieren Sie das Kontrollkästchen neben dem Namen des Filters.
- Bei Änderungen in den Einstellungen der Netzwerkfilter oder beim Erstellen neuer Filter wird eine Meldung in der Statusleiste angezeigt, dass die Filter geändert, aber noch nicht angewendet wurden. Die geänderten oder neuen Filter treten erst dann in Kraft, wenn Sie auf die Schaltfläche **Übernehmen** klicken und die Übernahme der Änderungen innerhalb von 30 Sekunden bestätigen.

  Wenn die neuen Filtereinstellungen nicht gespeichert werden sollen, klicken Sie auf die Schaltfläche **Abbrechen**. In diesem Fall werden die Filtereinstellungen auf den Zustand zurückgesetzt, der vor dem Durchführen der Änderungen wirksam war.

  Bei Bedarf können alle vorgenommen Änderungen abgelehnt und vorkonfigurierte Filter wiederhergestellt werden.

Allgemeine Informationen über Objektgruppen

Objektgruppen dienen dazu, die Definition von Netzwerkfiltern und Regeln der Adressenübersetzung im Programm ViPNet Monitor zu vereinfachen. In Objektgruppen werden mehrere Objekte eines Typs zusammengefasst, wodurch sie beim Einstellen der Filter- oder Regelparameter anstatt einzelner konkreter Objekte verwendet werden können.

Objektgruppen werden in mehrere Typen unterteilt:

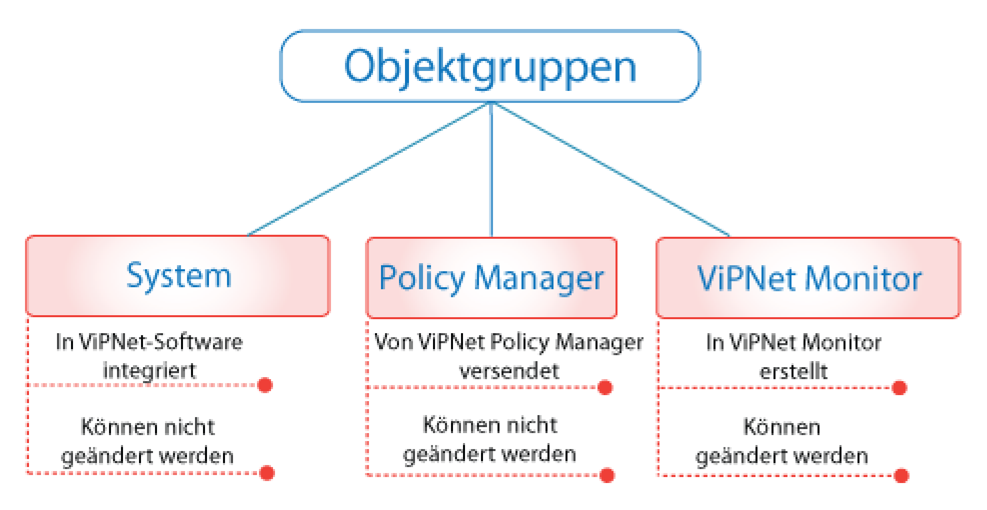


Abbildung 160. Typen von Objektgruppen

System-Objektgruppen repräsentieren mehrere im Programm ViPNet Policy Manager integrierte Objekte mit vorgegebenen Namen. Diese Objektgruppen können in neu zu erstellenden Netzwerkfiltern zur Angabe der Absender und Empfänger von IP-Paketen sowie in anderen benutzerdefinierten Objektgruppen verwendet werden. System-Objektgruppen werden in Gruppenlisten nicht angezeigt und können nicht geändert oder gelöscht werden.

Objektgruppen sind die Gruppen, die im Programm ViPNet Policy Manager erstellt werden. Diese Objektgruppen können nicht geändert oder in neu zu erstellenden Netzwerkfiltern, Regeln der Adressenübersetzung oder anderen benutzerdefinierten Objektgruppen verwendet werden. Im Programm ViPNet Monitor kann der Inhalt dieser Gruppen lediglich angezeigt werden.

Benutzer-Objektgruppen umfassen Gruppen von Objekten, die vom Benutzer unmittelbar im Programm ViPNet Monitor erstellt werden, sowie einige standardmäßig definierte Objektgruppen. Jede Objektgruppe wird unterschiedlich zusammengestellt, dabei können für jeden Gruppeninhalt mehrere Ausnahmen definiert werden. In die Inhalts- und Ausnahmeliste einer Gruppe können andere Objektgruppen desselben Typs oder bestimmte System-Objektgruppen eingeschlossen werden. Mit benutzerdefinierten Objektgruppen wird im Programm ViPNet Monitor im Bereich **Objektgruppen** gearbeitet.

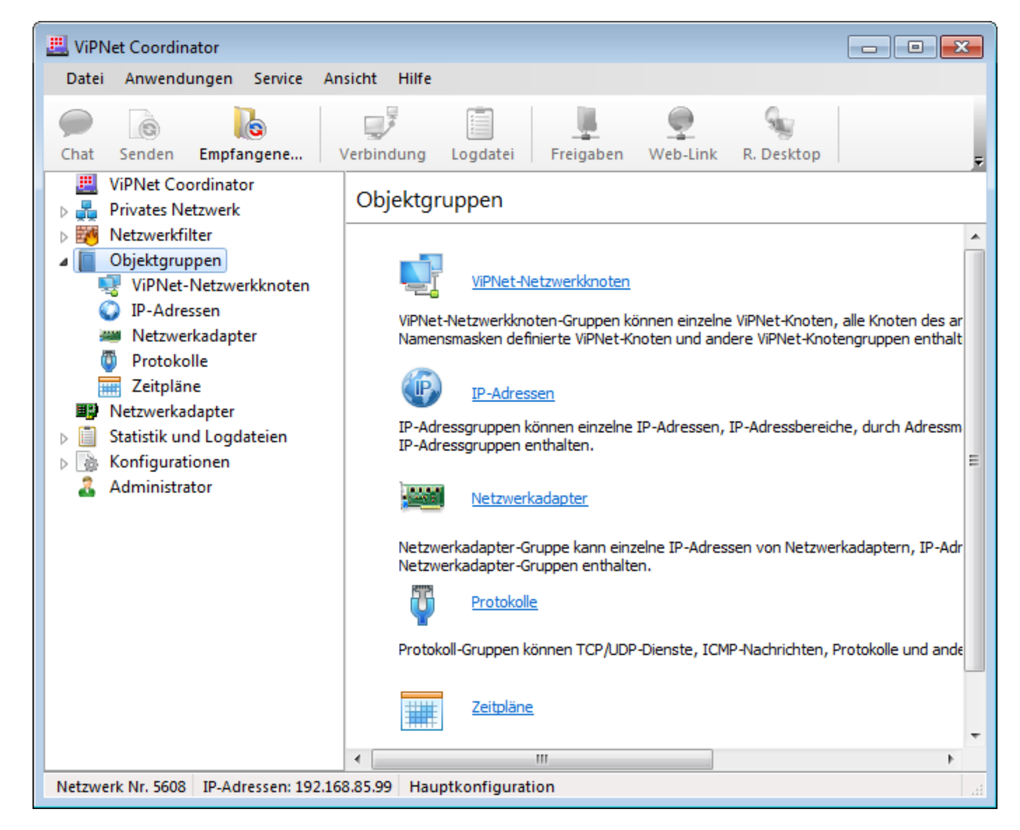


Abbildung 161. Verwaltung von Benutzer-Objektgruppen

Benutzer-Objektgruppen werden in folgende Kategorien unterteilt:

- **ViPNet Knoten**: Gruppe von Knoten im geschützten Netzwerk. Wird in Filtern des geschützten Netzwerks und der getunnelten Knoten verwendet.
- **IP-Adressen**: eine beliebige Kombination einzelner IP-Adressen und IP-Adressbereiche oder DNS-Namen. Wird in NAT-Regeln und Netzwerkfiltern verwendet (mit Ausnahme der Filter des privaten Netzwerks).
- **Netzwerkadapter**: eine beliebige Kombination einzelner Netzwerkadapter oder IP-Adressen der Netzwerkadapter. Wird in Netzwerkfiltern auf Coordinatoren verwendet (mit Ausnahme der Filter des privaten Netzwerks)
- **Protokolle**: eine beliebige Kombination von Protokollen und Ports. Wird in allen Filtern und NAT-Regeln verwendet.
- **Zeitpläne**: eine beliebige Kombination von Anwendungsregeln für Netzwerkfilter gemäß Uhrzeit und Wochentag. Wird in allen Filtern verwendet.

Praktisches Beispiel für die Verwendung von Objektgruppen und Netzwerkfiltern

Betrachten wir das folgende Beispiel für die Anwendung von Objektgruppen und Netzwerkfiltern. Nehmen wir an, innerhalb der Firma wird ein Mailserver verwendet, auf dem das Programm ViPNet Monitor installiert ist. Über diesen geschützten Mailserver werden die folgenden Funktionen abgewickelt:

- Austausch von E-Mail-Nachrichten mit externen Mailservern;
- Senden und Empfangen von E-Mail-Nachrichten über das Internet für Mitarbeiter, die von ihren Remote-Arbeitsplätzen arbeiten.

Die Nachrichten der externen Mailserver und der Remote-Benutzer werden über das SMTP-Protokoll an den internen Mailserver übermittelt. Für den Empfang von E-Mail-Nachrichten verwenden die Benutzer die Protokolle POP3 und IMAP.

Damit der Austausch von Nachrichten mit externen Mailservern und der Zugang der Benutzer zu ihren E-Mail-Nachrichten über das Internet sichergestellt werden können, sollte auf dem geschützten Mailserver ein Netzwerkfilter konfiguriert werden, der den Empfang und die Weiterleitung von IP-Paketen über Port 25 (Standardport für das SMTP-Protokoll) bzw. über Ports 110 und 143 (Standardport für das POP3- bzw. IMAP-Protokoll) des TCP-Protokolls ermöglicht.

Sie können eine Protokoll-Gruppe erstellen, die alle weiter oben erwähnten Protokolle beinhaltet. Diese Gruppe können Sie anschließend beim Erstellen des Netzwerkfilters verwenden. Außerdem können Sie diese Protokoll-Gruppe in weiteren Filtern für den Mailserver verwenden, falls solche Filter im Weiteren benötigt werden.

Führen Sie die folgenden Schritte aus, um eine Protokoll-Gruppe zu erstellen:

1 Wählen Sie im Programmfenster von ViPNet Monitor in der Navigationsleiste den Bereich **Objektgruppen** > **Protokolle**.

2 Klicken Sie in der Panel-Ansicht auf die Schaltfläche **Erstellen** und fügen im Optionenfenster der neuen Protokoll-Gruppe im Bereich **Inhalt** alle erforderlichen Protokolle hinzu.

3 Zum Hinzufügen des SMTP-Protokolls klicken Sie im Menü der Schaltfläche **Hinzufügen** auf den Eintrag **TCP/UDP-Protokoll** und geben im eingeblendeten Fenster die folgenden Werte an:

   - Protokoll: **TCP**
   - Quellport: **Alle Ports**
   - Zielport: Portnummer **25-smtp**

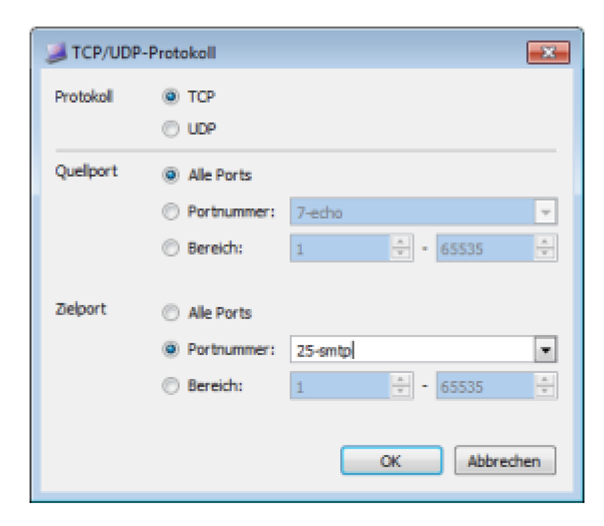


Abbildung 162. Beispiel für das Hinzufügen des SMTP-Protokolls zur Protokoll-Gruppe

4 Fügen Sie die Protokolle POP3 und IMAP auf die gleiche Weise hinzu, indem Sie für den Zielport die Portnummer 110 bzw. 143 auswählen.

5 Nachdem Sie alle benötigten Ports im Optionenfenster der Gruppe hinzugefügt haben, klicken Sie auf **OK**.

Es wird eine Protokoll-Gruppe angelegt. Verwenden Sie diese Gruppe beim Erstellen des Filters.

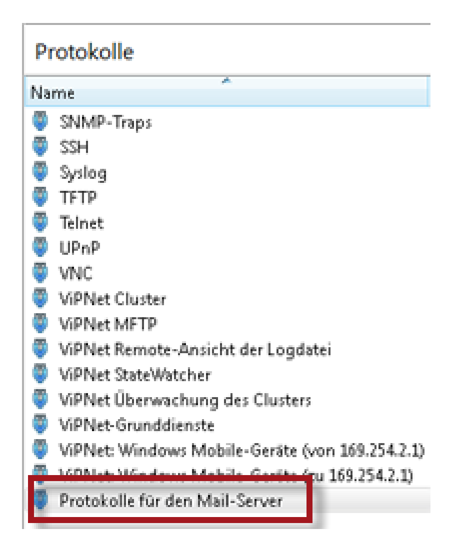


Abbildung 163. Neue Protokoll-Gruppe für den Mailserver fertiggestellt

Führen Sie auf dem geschützten Mailserver die folgenden Schritte aus, um einen Netzwerkfilter für den Austausch von E-Mail-Nachrichten mit externen Servern und Benutzern zu erstellen:

1 Wählen Sie im Programmfenster von ViPNet Monitor in der Navigationsleiste den Bereich **Netzwerkfilter** > **Offenes Netzwerk** (in ViPNet Client) oder den Bereich **Netzwerkfilter** > **Lokale Filter des offenen Netzwerks**.

2 Erstellen Sie im Bereich **Offenes Netzwerk** (in ViPNet Client) oder im Bereich **Lokale Filter des offenen Netzwerks** (in ViPNet Coordinator) einen Netzwerkfilter für alle IP-Adressen, da die IP-Adressen der externen Mailserver im Vorhinein nicht bekannt sind, und der neue Filter die IP-Adressen aller Benutzer erfassen sollte. Klicken Sie dazu in der Panel-Ansicht auf die Schaltfläche

Erstellen und legen im eingeblendeten Fenster der Filteroptionen die Parameter des neuen Filters fest.

3 Wählen Sie im Bereich **Allgemeine Optionen** in Gruppe **Aktion** die Option **IP-Traffic erlauben**.

4 Damit alle IP-Adressen vom Filter erfasst werden, dürfen in den Bereichen **Quellen** und **Ziele** keine Absender oder Empfänger definiert werden.

5 Klicken Sie im Bereich **Protokolle** im Menü der Schaltfläche **Hinzufügen** auf den Eintrag **Protokoll-Gruppe** und wählen im eingeblendeten Fenster die zuvor erstellte Protokoll-Gruppe aus.

6 Das Erstellen eines Zeitplans ist für diesen Filter nicht nötig.

7 Klicken Sie auf **OK**.

Der benötigte Netzwerkfilter wird erstellt.

Auf diese Weise wird auf dem geschützten Mailserver der Austausch von Nachrichten mit externen Servern und Mitarbeitern sowie der Zugang der Mitarbeiter zu ihren E-Mail-Nachrichten sichergestellt.

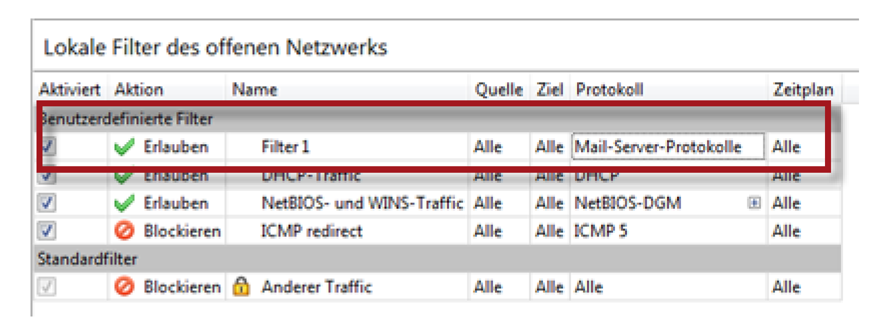


Abbildung 164. Erlaubender Filter für die Protokolle SMTP, POP3, IMAP fertiggestellt

Antispoofing

Das Programm ViPNet Coordinator verfügt über die Anti-Spoofing-Funktion, d.h. alle eingehenden IP-Pakete von auf einem gegebenen Netzwerkadapter nicht zugelassenen Absenderadressen werden blockiert. Antispoofing wird nur für offenen Traffic verwendet, weil für geschützten Datenverkehr die IP-Adresse des Absenders keine Rolle spielt. Ein offenes Paket wird erst durch das Antispoofing-System überprüft und danach entsprechend den Filtern (s. Grundprinzipien der Traffic-Filterung auf S. 271).

Mittels der Antispoofing kann für jeden Netzwerkadapter ein IP-Adressen Bereich bestimmt werden, von welchem alle Pakete durchgelassen werden sollen. Dadurch werden Pakete von IP-Adressen, die sich nicht im erlaubten Adressenbereich befinden, blockiert.

Wie es der Name schon verrät, ist die Aufgabe des Antispoofing der Schutz vor so genanntem Spoofing, eine der bekannten Netzwerkattacken. Beim Spoofing sendet der Angreifer ein IP-Paket an den angegriffenen Computer, in dem als Absenderadresse nicht die IP-Adresse des Angreifers, sondern die IP-Adresse eines anderen Knotens angegeben ist, für den die Verbindung zum angegriffenen Computer erlaubt ist. So könnte z.B. ein offenes Internet-Paket über den Coordinator durchgelassen werden, wenn statt der richtigen Absenderadresse eine Adresse eines internen privaten mit dem Coordinator verbundenen Computers eingegeben wird. Die Antispoofing-Regeln schließen diese Möglichkeit aus.

Zur Gewährleistung eines hohen Sicherheitsgrads eines Netzwerks wird es empfohlen, auf dem Coordinator Antispoofing zu aktivieren. Standardmäßig ist Antispoofing deaktiviert.

Um Antispoofing zu aktivieren, gehen Sie wie folgt vor:

1 Wählen Sie im Fenster des Programms ViPNet Monitor im Menü **Service** den Eintrag **Anwendungseinstellungen**.

2 Aktivieren Sie im Bereich **Traffic-Steuerung** das Kontrollkästchen **Antispoofing**.

3 Klicken Sie auf **Übernehmen**.

Auf Basis der Routingtabelle des Netzwerkknotens werden dadurch automatisch Antispoofing-Filter erstellt. Bei komplexen Routingmodellen (unter Verwendung von Routingmetriken oder asymmetrischen Routen) kann es zu Problemen in der Anwendung von Antispoofing kommen. In diesem Fall sollte Antispoofing wieder deaktiviert werden.

Antispoofing-Regeln werden ausschließlich für den offenen Traffic erstellt. Dabei wird der folgende Algorithmus verwendet:

- Auf allen Netzwerkadaptern mit Ausnahme des Standardadapters werden alle Quell-IP-Adressen blockiert, die nicht mit den Adressen übereinstimmen, die durch jeweiligen Adapter geroutet werden.
- Für einen Netzwerkadapter, der in der Standardroute angegeben ist, werden Quell-IP-Adressen blockiert, die mit den registrierten Routen anderer Adapter übereinstimmen.

Deaktivieren des Traffic-Schutzes

Sie können, wenn nötig, den Traffic-Schutz mit Hilfe der Software ViPNet Network Manager wieder deaktivieren. In diesem Fall wird jede Verarbeitung des Traffics und die Protokollierung der Pakete in der Logdatei der registrierten IP-Pakete deaktiviert. Das Herstellen von Verbindungen zu geschützten ViPNet Knoten wird nicht mehr möglich sein. Außerdem wird es nicht möglich sein, das Programm ViPNet SafeDisk-V zu starten, falls Sie dieses Programm gemeinsam mit ViPNet Monitor verwenden.

Deaktivieren des IP-Traffic-Schutzes wird für das Programm ViPNet Client Monitor im Administratormodus durchgeführt.



Achtung! Es wird davon abgeraten, auf einem Netzwerkknoten zu arbeiten, auf dem der Traffic-Schutz deaktiviert wurde, da der Computer in diesem Fall vor unberechtigten Zugriffen aus dem Netzwerk nicht mehr geschützt wird. Es ist ratsam, den Traffic-Schutz nur für kurze Zeiträume zu Testzwecken zu deaktivieren.

Führen Sie die folgenden Schritte aus, um den Traffic-Schutz zu deaktivieren:

1 Wählen Sie im Menü **Datei** den Befehl **Konfigurationen** > **Schutz deaktivieren**.

2 Wenn Sie möchten, dass nach der Deaktivierung des Traffic-Schutzes der Schutz unter bestimmten Bedingungen wieder automatisch aktiviert wird, gehen Sie im Fenster **Schutz deaktivieren** folgendermaßen vor:

- Aktivieren Sie das Kontrollkästchen **IP-Traffic-Schutz automatisch aktivieren**.
- Wählen Sie eine Bedingung zur automatischen Aktivierung des Traffic-Schutzes aus der Liste unter dem Kontrollkästchen aus: nach Neustart des Computers oder nach Ablauf einer bestimmten Zeitspanne.

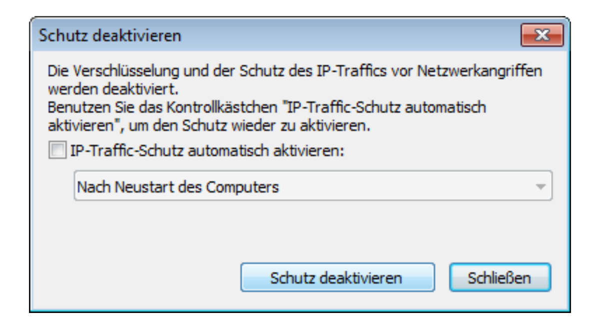


Abbildung 165. Deaktivierung des Traffic-Schutzes

3 Klicken Sie auf die Schaltfläche **Schutz deaktivieren**. Der Schutz des Traffics wird deaktiviert, das Programmsymbol von ViPNet Monitor in der Taskleiste nimmt das folgende Aussehen an:

4 Wählen Sie im Menü **Datei** den Befehl **Konfigurationen** > **Schutz aktivieren**.

Sperre des IP-Traffics

Mit Hilfe des Programms ViPNet Monitor können Sie den gesamten IP-Traffic des Computers sperren. In diesem Fall werden alle Verbindungen mit geschützten oder offenen Knoten blockiert. Sperre des IP-Traffics wird für das Programm ViPNet Client Monitor im Administratormodus durchgeführt.

Führen Sie die folgenden Schritte aus, um den IP-Traffic zu blockieren:

1 Im Programm ViPNet Monitor können Sie die Blockierung auf eine der folgenden Arten aktivieren:
   - Wählen Sie im Hauptfenster im Menü **Datei** den Befehl **Konfigurationen** > **IP-Traffic sperren**.
   - Klicken Sie in der Taskleiste mit der rechten Maustaste auf das und wählen im Menü den Eintrag **IP-Traffic sperren**.

2 Wenn Sie möchten, dass nach der Aktivierung der Sperre der Traffic unter bestimmten Bedingungen wieder automatisch entsperrt wird, gehen Sie im Fenster **IP-Traffic blockieren** folgendermaßen vor:
   - Aktivieren Sie das Kontrollkästchen **IP-Traffic automatisch erlauben**.
   - Wählen Sie eine Bedingung zur automatischen Aufhebung der Sperre aus der Liste unter dem Kontrollkästchen aus: nach Neustart des Computers oder nach Ablauf einer bestimmten Zeitspanne.

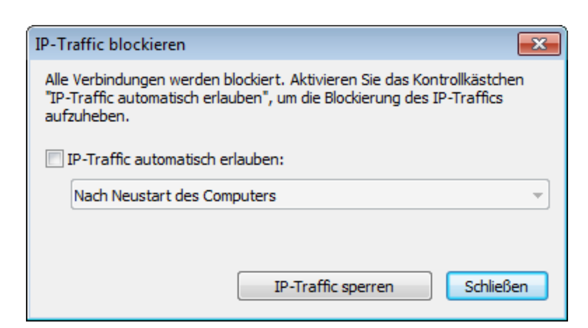


Abbildung 166. Aktivierung der Sperre des IP-Traffics

3 Klicken Sie auf die Schaltfläche **IP-Traffic sperren**. Der gesamte offene und verschlüsselte Traffic des Computers wird blockiert. Das Programmsymbol von ViPNet Monitor in der Taskleiste nimmt das folgende Aussehen an: .

4 Wählen Sie zum Aufheben der Sperre des IP-Traffics im Hauptfenster im Menü **Datei** den Eintrag **Konfigurationen** > **IP-Traffic erlauben**.



Übersetzung von IP-Adressen (NAT)

Wozu wird Adressenübersetzung verwendet?

Die Übersetzung der Netzwerkadressen (NAT, Network Address Translation) ist ein Verfahren zur Konvertierung von IP-Adressen eines Netzwerks in IP-Adressen eines anderen Netzwerks. Die Grundsätze der Technologie der Adressenübersetzung werden durch RFC 2663 geregelt http://tools.ietf.org/html/rfc2663.

NAT wird oft bei zwei Hauptaufgaben angewendet:

- Wenn eine Verbindung des lokalen Netzwerks mit dem Internet nötig ist, wobei die Anzahl der Knoten im lokalen Netzwerk die Anzahl der vom Provider bereitgestellten öffentlichen IP-Adressen überschreitet. NAT ermöglicht den Zugang zu Internet-Ressourcen von lokalen Netzwerken, die private IP-Adressen nutzen (s. Private IP-Adresse auf S. 372).

  Zur Lösung dieser Aufgabe wird die Quellübersetzung verwendet (s. Quellübersetzung auf S. 289).

- Für den Zugang zu internen Ressourcen aus einem öffentlichen Netzwerk. Durch den Einsatz der NAT-Technologie können lokale Netzwerke, die private Adressen besitzen, für Internetnutzer mit öffentlichen IP-Adressen zugänglich sein.

  Zur Lösung dieser Aufgabe wird die Zielübersetzung verwendet (s. Zielübersetzung auf S. 288).

Die NAT-Regeln werden auf einem Computer eingerichtet, der lokale (internen) Netzwerke und globale (öffentliche) Netzwerke (z.B. Internet) voneinander abgrenzt. Dieser Computer muss mindestens über zwei Netzwerkadapter verfügen:

- einen öffentlichen Adapter, der eine öffentliche IP-Adresse hat und den Zugang zum Internet gewährleistet;
- einen internen Adapter, der eine private IP-Adresse besitzt.

Die Übersetzung der Netzwerkadressen wird für IP-Pakete durchgeführt, die auf dem Weg vom internen in das externe Netzwerk oder umgekehrt die Firewall passieren.

Übersetzung von Adressen in der ViPNet Technologie



Achtung! In diesem Abschnitt beschriebene Übersetzungsregeln gelten ausschließlich für offenen Traffic. Bei verschlüsselten Traffic wirken andere Übersetzungsverfahren, die keine benutzerdefinierten Einstellungen verwenden, sondern automatisch eingestellt werden.

Ein ViPNet Netzwerkknoten mit dem Software ViPNet Network Manager kann über zwei Arten der NAT-Funktion (s. Netzwerkadressenübersetzung (NAT) auf S. 371) verfügen:

- Zielübersetzung gewährleistet eine Zuordnung von öffentlichen IP-Adressen oder Ports und privaten IP-Adressen oder Ports des internen Netzwerks. Diese Art der NAT ist dann anzuwenden, wenn ein interner Knoten aus einem äußeren Netzwerk über eine permanente Adresse zugänglich sein soll (z.B. ein Web-Server).
- Quellübersetzung (Masquerading) gewährleistet eine Zuordnung zwischen mehreren privaten Adressen eines lokalen Netzwerks und einer öffentlichen Adresse des Routers durch dynamische Zuweisung einmaliger Zusatzparameter (z.B. Ports). Dieser NAT-Typ wird verwenden, um mehreren Computern eines lokalen Netzwerks, die über private IP-Adressen verfügen, den Zugang zum Internet über einen Coordinator, der nur eine öffentliche Adresse besitzt, zu gewährleisten. Auf diese Weise können mehrere Computer des lokalen Netzwerks gleichzeitig eine öffentliche IP-Adresse nutzen.
- Gleichzeitige Übersetzung von Quell- und Zieladressen. Diese Form von NAT ermöglicht es, den Datenaustausch zwischen zwei Netzwerksegmenten so zu gestalten, dass die Knoten des einen Segments für die Knoten des zweiten Segments über die IP-Adresse Ihres Coordinators (wie bei der Zielübersetzung) zugänglich sind, und gleichzeitig die Pakete aus dem zweiten Segment an die Knoten des ersten Segments im Namen des entsprechenden Coordinator-Netzwerkadapters gesendet werden (wie bei der Quellübersetzung). Auf diese Weise werden die IP-Adressen der Knoten in einem Segment für das jeweils andere Segment verdeckt.

  Aktivieren Sie zum Erstellen einer Regel für die gleichzeitige Übersetzung von Quell- und Zieladressen im Bereich **NAT-Regeln** die beiden Kontrollkästchen **Quelladresse ersetzen durch** und **Zieladresse ersetzen durch** und geben Sie anschließend die erforderlichen Parameter an.

Damit die korrekte Funktionsweise einiger Anwendungsprotokolle (wie FTP, SIP) bei Verbindungen, die zwischen Client und Server unter Verwendung von NAT aufgebaut werden, gewährleistet werden kann, führt die Software ViPNet Network Manager eine zusätzliche Verarbeitung des Traffics durch. Diese zusätzliche Verarbeitung ermöglicht die Übersetzung von IP-Adressen, die manche Anwendungsprotokolle im Rumpf des IP-Pakets übermitteln (s. Konfiguration der Bearbeitungsparameter von Anwendungsprotokollen auf S. 296).

Zielübersetzung

Die Übersetzung der IP-Adresse des Zielknotens wird benötigt, um den Zugang aus dem Internet auf diejenigen Server des lokalen Netzwerks zu ermöglichen, die über keine eigene öffentliche IP-Adresse verfügen. Die NAT-Regel für die Übersetzung der Zieladresse ordnet den privaten IP-Adressen der lokalen Knoten die öffentliche IP-Adresse des Coordinators zu. In Übereinstimmung mit der NAT-Regel werden die öffentlichen Ziel-IP-Adressen (oder IP-Adressen und Ports) im Kopf der IP-Pakete durch private IP-Adressen des lokalen Netzwerks ersetzt. Auf diese Weise können externe Benutzer einen Zugang zu Objekten im lokalen Netzwerk über die öffentliche IP-Adresse erhalten.

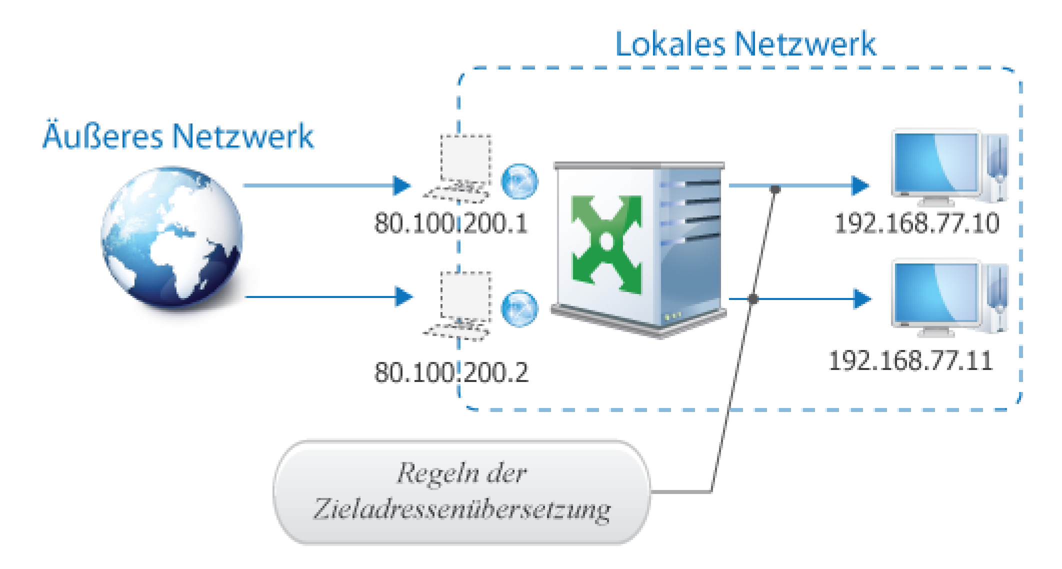


Abbildung 167. Zugang zu internen Ressourcen mit Hilfe der Zielübersetzung

Beim Erstellen einer Zielübersetzungsregel wird einer lokalen IP-Adresse eine öffentliche Adresse zugeordnet. Über diese öffentliche IP-Adresse kann das lokale Objekt von externen Benutzern angesprochen werden.

Wenn auf irgendeinen externen Netzwerkadapter aus dem Internet zugegriffen wird, überprüft der ViPNet Coordinator, ob für die gegebene IP-Adresse eine NAT-Regel definiert ist. Wenn es die Zielübersetzungsregel gibt, dann wird die Paketübertragung folgendermaßen durchgeführt:

- Der Coordinator ersetzt die öffentliche Empfänger-IP-Adresse in jedem Paket, das von einem externen Knoten weitergeleitet wurde, durch eine lokale Adresse in Übereinstimmung mit der Regel. Anschließend wird das Paket über den internen Netzwerkadapter an den Zielknoten innerhalb des lokalen Netzwerks weitergeleitet.
- Beim Eintreffen der Antwortpakete (im Rahmen einer bereits vorhandenen Sitzung) wird vom Coordinator die umgekehrte Substitution der Adressen durchgeführt. Die Adresse des lokalen Knotens wird durch die öffentliche IP-Adresse des externen Netzwerkadapters auf dem Coordinator ersetzt. Anschließend wird das Antwortpaket an sein Ziel (Knoten im Internet) weitergeleitet

  Auf diese Weise sieht es bei der Paketübertragung im Internet so aus, als ob sowohl der Absender als auch der Empfänger des Pakets über öffentliche IP-Adressen verfügen würden.



Achtung! Bei der Zielübersetzung kann die Verbindung nur von einem externen Knoten initiiert werden. Damit auch ein lokaler Knoten einen Zugang zum Internet hat (zweiseitiges NAT), sollte neben der Zielübersetzungsregel auch die Quellübersetzungsregel definiert werden.

Quellübersetzung

Die Quellübersetzung der IP-Adresse wird benötigt, um lokalen Computern den Zugang zum Internet zu ermöglichen. Die NAT-Regel für die Übersetzung der Quelladresse ordnet einigen privaten IP-Adressen lokaler Knoten die öffentliche IP-Adresse des Coordinators zu. In Übereinstimmung mit der NAT-Regel werden die privaten Quell-IP-Adressen im Kopf der IP-Pakete durch die öffentliche IP-Adresse des Coordinators ersetzt. Auf diese Weise können Knoten des lokalen Netzwerks Verbindungen zu Knoten im Internet im Namen der öffentlichen IP-Adresse des Coordinators herstellen.

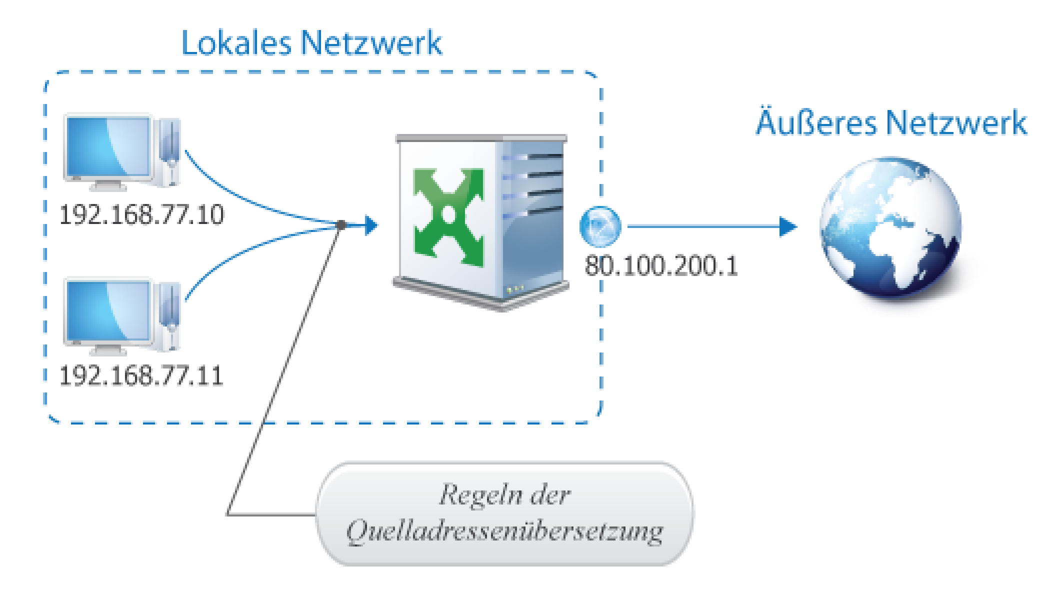


Abbildung 168. Zugang zum Internet mit Hilfe der Quellübersetzung

Wenn auf dem Coordinator die Quellübersetzung von IP-Adressen konfiguriert ist, dann werden alle Transit-IP-Pakete, die den Coordinator auf dem Weg vom lokalen Netzwerk in das Internet (oder andere globale Netzwerke) passieren, auf die folgende Weise verarbeitet:

- Zum Zeitpunkt der Übertragung eines IP-Pakets aus dem lokalen Netzwerk in das Internet werden die Absenderadresse und (oder) der Absenderport für die TCP- und UDP-Protokolle durch den ViPNet Coordinator umgewandelt. Bei Paketen des ICMP-Protokoll wird die Absenderadresse umgewandelt, alle anderen Parameter werden gespeichert. Die private Adresse des Paketabsenders wird durch die öffentliche Adresse des externen Netzwerkadapters auf dem Coordinator ersetzt, der den Zugang zum öffentlichen Netzwerk gewährleistet. Während der weiteren Übertragung im Internet beinhaltet das Paket die öffentliche IP-Adresse des Absenders. Die Absenderportnummern (für die TCP- und UDP-Protokolle) und andere gespeicherte Parameter (für das ICMP-Protokoll) des Pakets sind für alle ausgehenden Verbindungen des externen Netzwerkadapters des Coordinators einmalig. Nach der Umwandlung wird das Paket an den Empfänger über das Internet weitergeleitet.

- Beim Eintreffen der Antwortpakete führt der ViPNet Coordinator die entgegensetzte Umwandlung der angegebenen Parameter durch. Während der Übergabe eines Antwortpakets ersetzt der ViPNet Coordinator die Empfängeradresse durch die private Adresse des Knotens im lokalen Netzwerk, an den das Antwortpaket adressiert ist. Die Umwandlung erfolgt anhand der eindeutigen Portnummern, die den ausgehenden Paketen zugewiesen wurden (bei TCP- und UDP-Protokollen) sowie anhand der gespeicherten Parameter der ausgehenden Pakete (beim ICMP-Protokoll). Die Portnummern (bei TCP- und UDP-Protokollen) werden ebenfalls auf ihre ursprünglichen Werte zurückgesetzt. Danach werden die Antwortpakete über den internen Netzwerkadapter an den Zielknoten im lokalen Netzwerk weitergeleitet.



Hinweis. Für alle Protokolle mit Ausnahme von TCP, UDP und ICMP werden jeweils nur die IP-Adressen umgewandelt. Bei Protokollen mit teilweiser Umwandlung wird die Quellübersetzung nicht funktionieren, wenn mehrere lokale Netzwerkknoten gleichzeitig eine Verbindung zur ein und derselben IP-Adresse des öffentlichen Netzwerks initiieren.

Beispiel für die Verwendung der Netzwerkadressenübersetzung (NAT)

Betrachten wir das folgende Beispiel für die Verwendung von NAT: nehmen wir an, dass an der Grenze des lokalen Büronetzwerks ein Coordinator installiert ist, der als Firewall auftritt. Für die Benutzer des Subnetzwerks 192.168.2.0 soll der Zugang zum Internet über das HTTP- und HTTPS-Protokoll sichergestellt werden. Dazu sollte auf dem Coordinator eine NAT-Regel für Quelladressen (s. Quellübersetzung auf S. 289) konfiguriert werden. Zusätzlich sollte ein Transit-Filter definiert werden, der die Weiterleitung des Traffics aus dem lokalen Netzwerk in das Internet erlaubt.

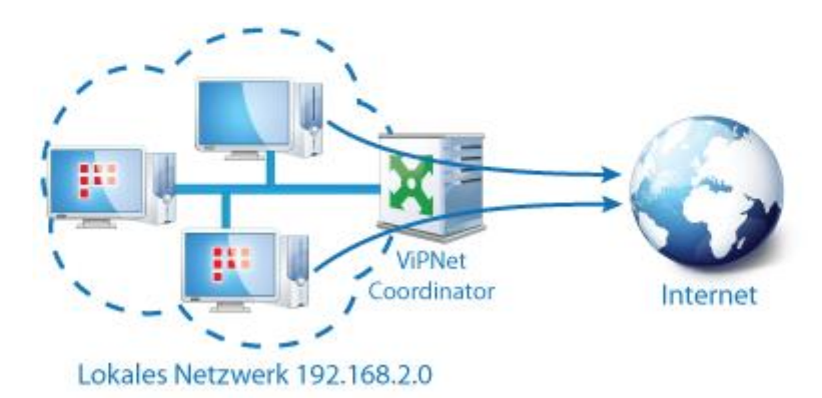


Abbildung 169. Einrichtung des Internetzugangs

Führen Sie im Programm ViPNet Coordinator die folgenden Schritte aus, um den Benutzern des lokalen Netzwerks den Zugang zum Internet bereitzustellen:

1 Wählen Sie im Programm ViPNet Monitor in der Navigationsleiste den Bereich **Netzwerkfilter** > **NAT-Regeln** und erstellen eine Regel der Quellübersetzung, indem Sie folgende Parameter definieren:

- Fügen Sie im Bereich **Quellen** die Adresse des Subnetzwerks 192.168.2.0 und die Maske 255.255.255.0 hinzu.
- Fügen Sie im Bereich **Ziele** die IP-Adressgruppe **Öffentliche IP-Adressen** hinzu. Diese Gruppe ist im Programm ViPNet Monitor standardmäßig eingestellt.
- Fügen Sie im Bereich **Protokolle** die folgenden Protokolle hinzu:
  - Protokoll: **TCP**, Quellport: **Alle Ports**, Zielport: **80-http**.
  - Protokoll: **TCP**, Quellport: **Alle Ports**, Zielport: **443-https**.
- Aktivieren Sie im Bereich **NAT-Regeln** das Kontrollkästchen **Quelladresse ersetzen durch** und wählen das Optionsfeld **IP-Adresse des ausgehenden Netzwerkadapters (wird automatisch festgelegt)** aus.

2 Klicken Sie im Bereich **NAT-Regeln** auf die Schaltfläche **Alle übernehmen**.

3 Wählen Sie in der Navigationsleiste den Bereich **Netzwerkfilter** > **Transit-Filter des offenen Netzwerks** und erstellen einen Netzwerkfilter, indem Sie die folgenden Parameter angeben:

- Wählen Sie im Bereich **Allgemeine Optionen** die Aktion **IP-Traffic erlauben**.
- Fügen Sie im Bereich **Quellen** die Adresse des Subnetzwerks 192.168.2.0 und die Maske 255.255.255.0 hinzu.
- Fügen Sie im Bereich **Ziele** die IP-Adressgruppe **Öffentliche IP-Adressen** hinzu. Diese Gruppe ist im Programm ViPNet Monitor standardmäßig eingestellt.
- Fügen Sie im Bereich **Protokolle** die folgenden Protokolle hinzu:
  - Protokoll: **TCP**, Quellport: **Alle Ports**, Zielport: **80-http**.
  - Protokoll: **TCP**, Quellport: **Alle Ports**, Zielport: **443-https**.

4 Klicken Sie im Bereich **Transit-Filter des offenen Netzwerks** auf die Schaltfläche **Alle übernehmen**.



Bearbeitung der Anwendungsprotokolle

Allgemeine Informationen über Anwendungsprotokolle

Die Funktionalität von Netzwerkdiensten wie IP-Telefonie, DNS- oder FTP-Dienst wird durch Anwendungsprotokolle gewährleistet, die das Übermitteln von IP-Adressen im Rumpf der IP-Pakete regeln. Dieses Verhalten kann zu Schwierigkeiten im Betrieb der aufgezählten Dienste führen, falls auf geschützten Objekten virtuelle IP-Adressen oder Adressenübersetzung verwendet wird. Außerdem bauen einige Protokolle neben einer Hauptverbindung (Kontrollverbindung) zusätzliche Verbindungen zu zufällig ausgewählten Ports auf, um Daten zu übertragen. Für IP-Pakete, die an einen Zielport weitergeleitet werden sollen, dessen Nummer im Vorhinein nicht bekannt ist, können keine erlaubenden Filter definiert werden. Dementsprechend wird eine solche Verbindung blockiert.

Die aufgezählten Probleme können durch die Verarbeitung von Anwendungsprotokollen gelöst werden:

- Substitution der virtuellen IP-Adresse im Paketrumpf durch die reelle IP-Adresse, falls die Technologie der virtuellen IP-Adressen verwendet wird.
- Substitution der IP-Adresse des geschützten Knotens im Anwendungsprotokoll durch die übersetzte IP-Adresse (bei Verwendung der Technologie der Adressenübersetzung).
- Aktivierung der erlaubenden Filterregel für zusätzliche Verbindungen zu zufällig ausgewählten Ports, die vom Anwendungsprotokoll geöffnet werden.



Hinweis. Im Programm ViPNet Monitor wird die Verarbeitung von Anwendungsprotokollen für alle Trafictypen ausgeführt: offen, geschützt und getunnelt.

Die Konfiguration der Verarbeitung der Anwendungsprotokolle wird für das Programm ViPNet Client Monitor im Administratormodus durchgeführt.

Es muss berücksichtigt werden, dass die Verarbeitung von Anwendungsprotokollen keine automatische Erlaubnis für den Aufbau von Kontrollverbindungen zu offenen Knoten bedingt. Das Herstellen von Kontrollverbindungen zu offenen Knoten wird in Übereinstimmung mit den konfigurierten Filtern des offenen Netzwerks und gemäß der im Programm ViPNet Monitor eingestellten Filtern des Traffic durchgeführt.

Beschreibung von Anwendungsprotokollen



Hinweis. Im Programm ViPNet Network Manager Version 3.2 und höher wurden die Web-Filter und die Verarbeitung des Anwendungsprotokolls HTTP herausgenommen.

Im Programm ViPNet Monitor besteht die Möglichkeit, Parameter für die Verarbeitung folgender Anwendungsprotokolle zu konfigurieren:

- FTP-Protokoll: gewährleistet die Übertragung von Dateien zwischen FTP-Client und FTP-Server.
- DNS-Protokoll (Domain Name System): gewährleistet die Auflösung der DNS-Namen von Netzwerkknoten in IP-Adressen.
- H.323-Protokoll: gewährleistet die Funktionalität von Anwendungen für die Durchführung von Videokonferenzen über IP-Netzwerke (inklusive Internet).
- SCCP-Protokoll (Skinny Client Control Protocol): gewährleistet die Übertragung von Nachrichten zwischen Skinny-Clients (drahtgebundene und drahtlose IP-Telefone von Cisco) und Voicemail-Server (Cisco Unity und Cisco Unified Communications Manager).
- SIP-Protokoll (Session Initiation Protocol): gewährleistet den Aufbau von Kommunikationssitzungen bei Übertragung von Gesprächen, Videogesprächen und Multimedia-Daten.



Hinweis. Die Liste der von ViPNet Monitor unterstützten Anwendungsprotokolle ist standardmäßig vorgegeben. Es können keine Protokolle in der Liste hinzugefügt oder entfernt werden.

Konfiguration der Bearbeitungsparameter von Anwendungsprotokollen



Achtung! In Netzwerken, in denen die Verarbeitung der Anwendungsprotokolle mit ViPNet Mitteln durchgeführt wird, sollte die DPI-Funktion (deep packet inspection, Tiefanalyse der Pakete) auf den Netzwerkgeräten (Router, Gateways) deaktiviert werden. Die Verwendung von DPI kann zu Störungen im Betrieb von Anwendungen führen, die Protokolle wie FTP, DNS, H.323, SCCP, SIP benutzen.

Führen Sie die folgenden Schritte aus, um die Verarbeitungsparameter der Anwendungsprotokolle für den offenen und verschlüsselten Traffic zu konfigurieren:

1 Wählen Sie im Fenster des Programms ViPNet Monitor im Menü **Service** den Eintrag **Anwendungseinstellungen**.

2 Wählen Sie im Fenster **Einstellungen** in der Navigationsleiste den Bereich **Anwendungsprotokolle**.

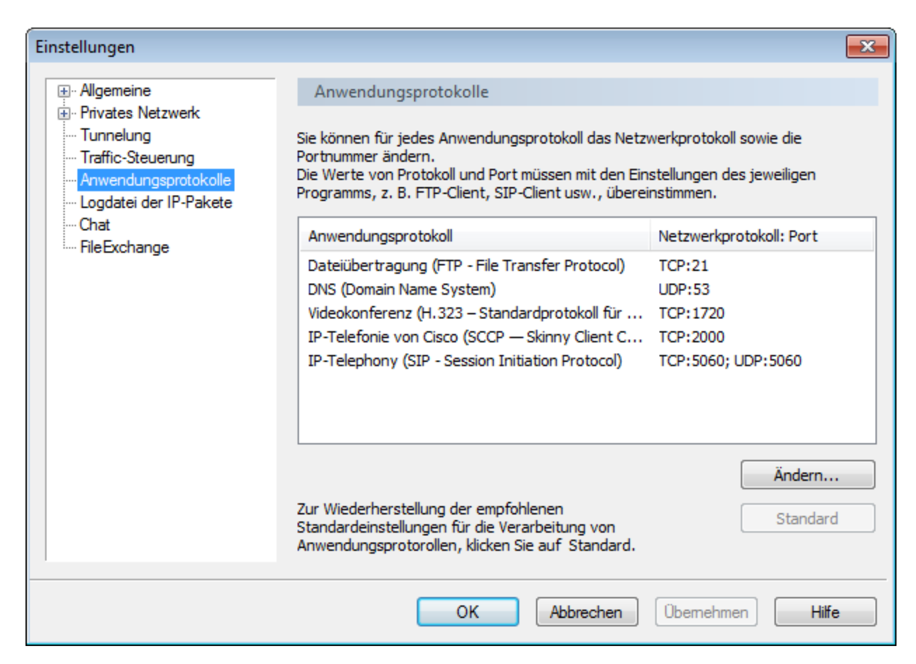


Abbildung 170. Parameter der Anwendungsprotokolle

Im Bereich **Anwendungsprotokolle** wird eine Liste der vom Programm unterstützten Anwendungsprotokolle angezeigt (s. Beschreibung von Anwendungsprotokollen auf S. 295).



Hinweis. Standardmäßig sind für alle Anwendungsprotokolle die am häufigsten verwendeten Netzwerkprotokolle und Ports angegeben.

Die Liste der von ViPNet Monitor unterstützten Anwendungsprotokolle ist standardmäßig vorgegeben. Es können keine Protokolle in der Liste hinzugefügt oder entfernt werden.

3 Wählen Sie im Bereich **Anwendungsprotokolle** das Protokoll aus, für das Sie die Verarbeitungsparameter modifizieren möchten, und klicken auf die Schaltfläche **Ändern**.

4 Wenn nötig, führen Sie im Fenster **Konfiguration des Anwendungsprotokolls: ...** (Name hängt vom gewählten Anwendungsprotokoll ab) die folgenden Schritte aus:

- Aktivieren Sie zum Einschalten eines Protokolls das entsprechende Kontrollkästchen und geben die Ports ein.



Hinweis. Die angegebenen Parameter für die Protokollverarbeitung sollten mit den Parametern in den Einstellungen des jeweiligen Programms, z. B. FTP-Client, DNS-Client, SIP-Client usw., übereinstimmen.

Bei Eingabe von Portnummern oder Portbereichen sollten diese durch Komma getrennt werden.

- Deaktivieren Sie zum Ausschalten eines Netzwerkprotokolls das entsprechende Kontrollkästchen.
- Zum Deaktivieren der Verarbeitung eines Anwendungsprotokolls:
  - Deaktivieren Sie alle Netzwerkprotokolle.
  - Klicken Sie im Fenster mit der Warnmeldung auf **OK**.

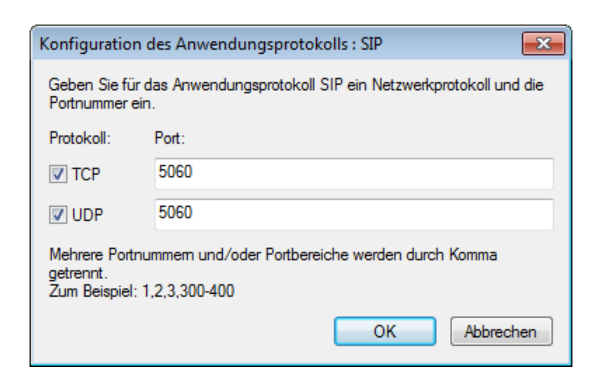


Abbildung 171. Konfiguration der Bearbeitungsparameter eines Anwendungsprotokolls

Klicken Sie nach Abschluss der Konfiguration auf **OK**.



Achtung! Es wird davon abgeraten, die Verarbeitung der Anwendungsprotokolle zu deaktivieren, da sonst die Arbeit der entsprechenden Anwendungen gestört werden könnte.

5 Klicken Sie zum Speichern der Einstellungen im Fenster **Einstellungen** auf die Schaltfläche **Übernehmen**.

Wenn Sie Standardeinstellungen wiederherstellen möchten, klicken Sie im Bereich **Anwendungsprotokolle** auf **Standard**.



Schutz des Traffics offener Netzwerkknoten (Tunnelung)

Allgemeine Informationen

Es tritt oft die Notwendigkeit auf, den Traffic zwischen zwei Netzwerkknoten an einem potenziell gefährlichen Netzwerkabschnitt zu schützen oder einen Knoten mit dem Netzwerk zu verbinden, auf dem keine ViPNet Software installiert werden kann oder soll. Eine solche Situation kann dann auftreten, wenn spezielle Geräte (z.B. IP-ATC und IP-Telefone) oder Server (SQL, 1C oder DHCP), auf denen die Installation zusätzlicher Software nicht gewünscht ist, an das Netzwerk angeschlossen werden sollen.

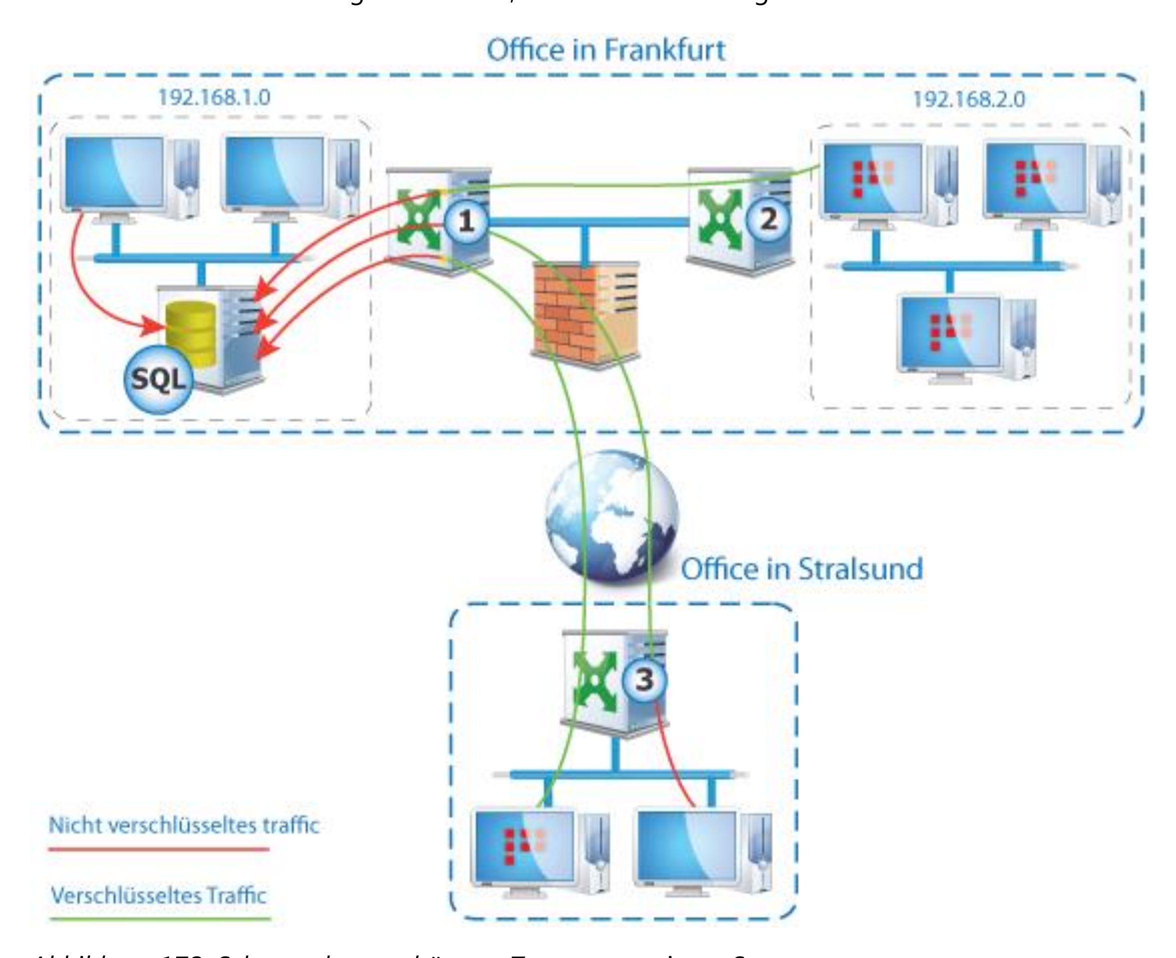


Abbildung 172. Schema des geschützten Zugangs zu einem Server

Für die Lösung dieser Aufgaben wird die Technologie der Tunnelung verwendet. Diese Technologie sieht vor, dass der Traffic eines Netzwerkknotens nicht mehr direkt an einen anderen Netzwerkknoten übermittelt wird. Stattdessen wird der Traffic über einen ViPNet Coordinator weitergeleitet, auf dem die Daten zunächst gefiltert und durch kryptografische Verfahren geschützt werden.

Bei Tunnelung wird der Traffic gemäß folgenden Regeln geschützt:

- Vom offenen Netzwerkknoten bis zu seinem tunnelnden Coordinator wird der Traffic unverschlüsselt übertragen.
- Auf dem Coordinator wird der Traffic gefiltert und verschlüsselt. Anschließend werden die Daten verschlüsselt entlang der Route weitergeleitet.

- Auf dem Coordinator, der den Netzwerkknoten des Empfängers tunnelt, wird der Traffic entschlüsselt und an den Zielknoten unverschlüsselt weitergeleitet.

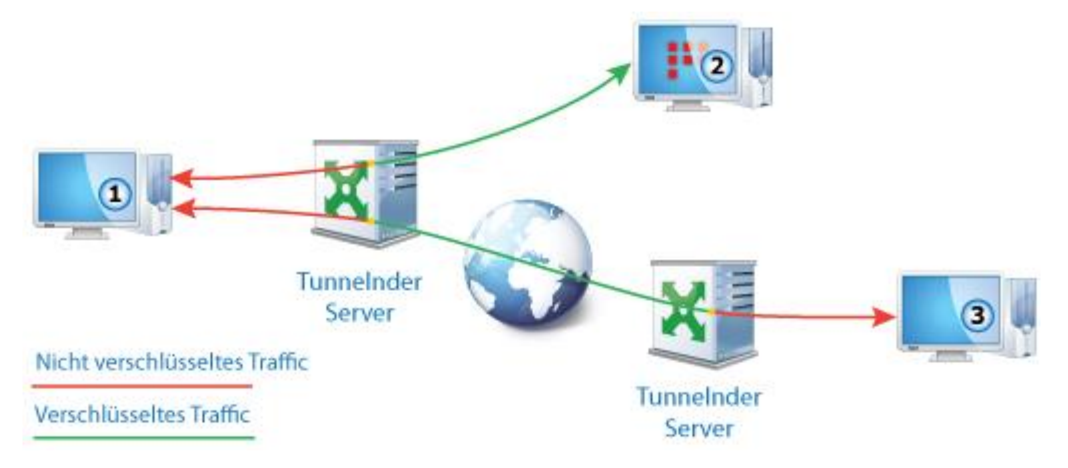


Abbildung 173. Tunnelarten im ViPNet

In ViPNet Terminologie wird die Verbindung zwischen Netzwerkknoten **1** und Netzwerkknoten **2** als ein „Halbtunnel", und die Verbindung zwischen Netzwerkknoten **1** und Netzwerkknoten **3** als ein „Volltunnel" bezeichnet.

In diesem Kapitel wird die Konfiguration der Tunnelung offener Netzwerkknoten durch den Coordinators behandelt. Die Konfiguration von ViPNet Netzwerkknoten, die mit den getunnelten Netzwerkobjekten kommunizieren sollen, wird im Abschnitt Konfiguration des Zugangs zu getunnelten Netzwerkobjekten (auf S. 265).

Konfiguration der Tunnelung

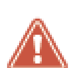
Führen Sie die folgenden Schritte aus, um die Tunnelung offener Knoten durch den Coordinator zu konfigurieren:

1. Geben Sie die IP-Adressen der offenen Knoten an, die getunnelt werden sollen.
2. Erstellen Sie Netzwerkfilter, wenn der Zugriff auf getunnelte Knoten eingeschränkt werden soll. Die Filter können unmittelbar auf dem Coordinator konfiguriert oder als Teil der entsprechenden Richtlinie aus dem Programm ViPNet Policy Manager an den Coordinator gesendet werden.

Zu tunnelnde Knoten können auf zwei Arten definiert werden:

- Im Programm ViPNet Network Manager. In diesem Fall werden die Adressen der getunnelten Knoten nach dem Versand neuer Adresslisten auch an den tunnelnden Coordinator sowie an alle Clients, die mit diesem Coordinator verbunden sind, übermittelt.

  Die erste Methode ist praktisch, da die Adressen für die Tunnelung zentralisiert angegeben werden. Wir empfehlen, diese Vorgangsweise zu verwenden. Die zweite Methode kann benutzt werden, wenn der Zugang zu getunnelten Adressen für eine geringe Anzahl an Clients eingerichtet werden soll.
- Im Programm ViPNet Monitor. In diesem Fall werden die Adressen der getunnelten Knoten auf dem tunnelnden Coordinator sowie auf allen Netzwerkknoten, die über einen Zugang zu den getunnelten Knoten verfügen sollen, definiert. Jene ViPNet Knoten, auf denen die getunnelten Adressen nicht angegeben werden, erhalten keinen Zugang zu den getunnelten Knoten.



Achtung! Bitte beachten Sie, dass Konfiguration der Adressen im ViPNet Network Manager alle zuvor vorgenommenen Einstellungen auf dem Coordinator oder den Clients überschreibt. Auf diesem Grund sollte von Anfang an eine Methode zur Festlegung von IP-Adressen ausgewählt werden, an die Sie sich bei nachfolgenden Rekonfigurationen des Netzwerks halten.

Festlegen der getunnelten Netzwerkobjekte

Führen Sie auf dem tunnelnden Coordinator die folgenden Schritte aus, um die IP-Adressen der für die Tunnelung bestimmten offenen Knoten anzugeben:

1. Wählen Sie im Programmfenster von ViPNet Monitor im Menü **Service** den Eintrag **Anwendungseinstellungen**.
2. Wählen Sie im Fenster **Einstellungen** den Bereich **Tunnlung**.

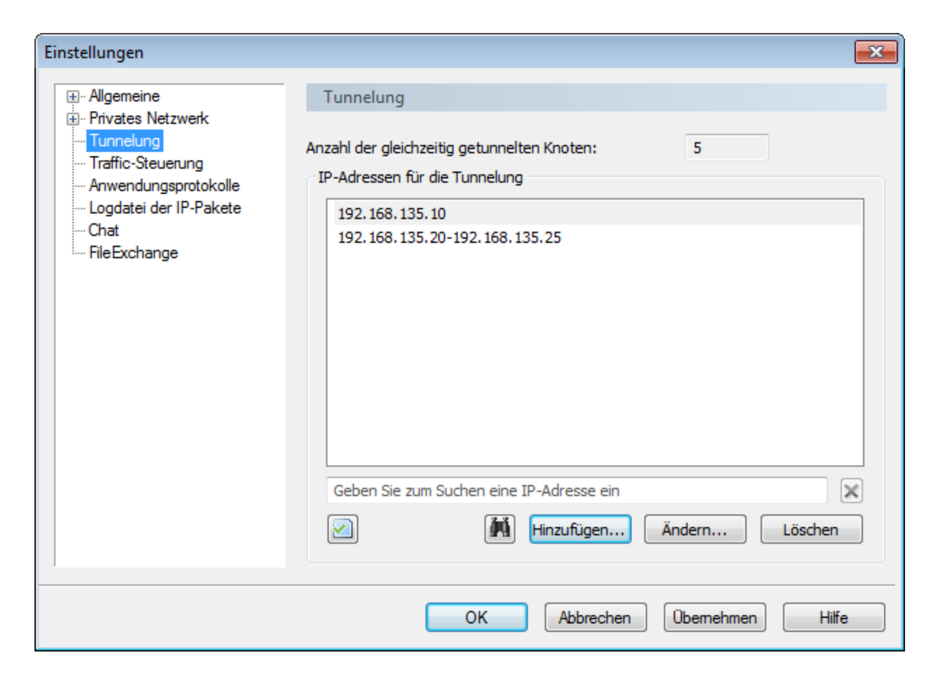


Abbildung 174. Hinzufügen von IP-Adressen zur Tunnelung im ViPNet Coordinator

3 Erstellen Sie mit Hilfe der entsprechenden Schaltflächen eine Liste von IP-Adressen der getunnelten Knoten.

Wenn Sie die IP-Adresse des getunnelten Knotens nicht kennen, können Sie die Adresse anhand des Computernamens ermitteln. Klicken Sie dazu auf die Schaltfläche und führen im eingeblendeten Fenster die Suche nach der benötigten IP-Adresse anhand des Computernamens durch.

Beim Hinzufügen der IP-Adresse wird automatisch überprüft, ob sich die angegebene Adresse mit den Adressen in der Liste oder mit den IP-Adressen anderer Netzwerkknoten (inklusive getunnelter Knoten) überschneidet. Diese Überprüfung dient dazu, das Hinzufügen von identischen IP-Adressen zu vermeiden. Wenn im Zuge der Überprüfung sich überschneidende Einträge festgestellt werden, wird eine entsprechende Fehlermeldung angezeigt. Beheben Sie die Überschneidung der IP-Adressen.

Sie können die Überprüfung auf eine mögliche Überschneidung der IP-Adressen auch manuell durchführen. Klicken Sie dazu auf die Schaltfläche .

4 Wenn Sie fertig sind, klicken Sie auf **OK**.

Nach dem Festlegen der IP-Adressen für die Tunnelung können Netzwerkfilter auf dem Coordinator konfiguriert werden, die den Zugriff auf getunnelte Knoten in Übereinstimmung mit bestimmten Parametern begrenzen. Damit die Benutzer anderer ViPNet Netzwerkknoten auf die getunnelten Knoten des gegebenen Coordinators zugreifen können, sollten die IP-Adressen dieser Knoten zusätzlich auf jedem betroffenen Netzwerkknoten angegeben werden (s. Konfiguration des Zugangs zu getunnelten Netzwerkobjekten auf S. 265).

Erforderliche Einstellungen auf getunnelten Knoten



Hinweis. Beim Planen der Netzwerkstruktur sollte berücksichtigt werden, dass die getunnelten Knoten (ohne ViPNet Software, jedoch mit geschütztem Zugang) hinter einem bestimmten Netzwerkadapter des Coordinators oder hinter einem separaten Coordinator untergebracht werden sollten. Dies ist sowohl aus Sicherheits- als auch aus praktischen Gründen bei der Verwaltung des ViPNet Netzwerks empfehlenswert.

Damit das Routing des Traffics zwischen den getunnelten Objekten und den geschützten ViPNet Knoten ordnungsgemäß funktioniert, müssen folgende Bedingungen erfüllt sein:

- Die getunnelten Knoten müssen sich im gleichen gerouteten Netzwerk wie der tunnelnde Coordinator befinden.
- IP-Pakete, die von getunnelten Knoten an geschützte ViPNet Knoten übermittelt werden, müssen durch den tunnelnden Coordinator weitergeleitet werden. Führen Sie dazu eine der folgenden Aktionen aus:
    - Legen Sie auf den getunnelten Netzwerkknoten den tunnelnden Coordinator als Standardgateway fest.
    - Definieren Sie auf den getunnelten Netzwerkknoten statische Routen für geschützte ViPNet Knoten über den tunnelnden Coordinator.

16

Konfiguration und Verwendung der Namensdienste DNS und WINS im ViPNet Netzwerk

DNS- und WINS-Dienste im ViPNet Netzwerk

Die Anwendungen in ViPNet Netzwerken können virtuelle IP-Adressen verwenden, die real im Netzwerk nicht existieren und für jeden Netzwerkknoten einmalig sind. Deswegen wird von ViPNet Software eine spezielle Bearbeitung der Protokolle von DNS- und WINS-Diensten durchgeführt.

Damit ein fehlerfreier Betrieb der DNS- und WINS-Dienste unter Verwendung von virtuellen Adressen im ViPNet Netzwerk gewährleistet werden kann, führt ViPNet Software automatisch eine spezielle Verarbeitung der IP-Pakete dieser Dienste durch. Diese Verarbeitung wird durchgeführt, um den Anwendungen auf den geschützten Knoten, die den DNS- oder WINS-Dienst benutzen, die korrekten IP-Adressen für den Zugriff auf andere geschützte und getunnelte Knoten (ob reell oder virtuell) bereitzustellen.

Wenn auf einem DNS-(WINS-)Server, der von solchen Anwendungen angesprochen wird, ViPNet Software installiert ist, oder wenn dieser Server vom Coordinator getunnelt wird, dann wird die Unterstützung von DNS- bzw. NetBIOS-Namen für virtuelle IP-Adressen ohne zusätzliche Einstellungen der ViPNet Software sichergestellt, falls bestimmte Regeln (s. DNS- bzw. WINS-Server auf dem geschützten oder getunnelten Knoten auf S. 307) eingehalten werden.

Die DNS-Namen für die geschützten Knoten können manuell im Programm ViPNet Monitor direkt auf dem Netzwerkknoten oder im Programm ViPNet Network Manager definiert werden. In diesem Fall stehen bei Verwendung des DNS-Dienstes zusätzliche Möglichkeiten zur Verfügung:

- Die sichere Kommunikation der Anwendungen mit entfernten geschützten ViPNet Knoten mit Hilfe von DNS-Namen und unter Verwendung offener (öffentlicher) DNS-Server (s. Ungeschützter DNS- bzw. WINS-Server auf S. 309) wird gewährleistet.
- Für einen geschützten ViPNet Knoten besteht die Möglichkeit, mit seinem Coordinator unter Verwendung von DNS-Namen zu kommunizieren. Dies geschieht durch Veröffentlichung der IP-Adresse, die dem Coordinator nicht fest zugeordnet ist (zum Beispiel die IP-Adresse für den Coordinatorzugang über ein NAT-Gerät), auf dem DNS-Server. Bei der automatischen Veröffentlichung der Zugangsadresse auf einem öffentlichen DNS-Server (die Technologie des dynamischen DNS, oder DYN DNS) kann ein abgesicherter Zugang zum Coordinator, dessen Zugangs-IP-Adresse sich dynamisch ändert, verwirklicht werden.

DNS- bzw. WINS-Server auf dem geschützten oder getunnelten Knoten

Besonderheiten bei Verwendung

Bei Verwendung eines DNS- bzw. WINS-Servers, der sich auf einem geschützten oder getunnelten Knoten befindet, sollten folgende Besonderheiten beachtet werden:

- Für die Sicherstellung der Funktionsfähigkeit der DNS- und WINS-Dienste müssen keine zusätzlichen Einstellungen in ViPNet Software vorgenommen werden.
- Wenn die DNS- bzw. NetBIOS-Namen mitsamt den entsprechenden IP-Adressen der geschützten und getunnelten Objekte automatisch auf dem DNS- bzw. WINS-Server registriert werden, dann gewährleistet die ViPNet Technologie eine automatische Veröffentlichung der erforderlichen reellen oder virtuellen IP-Adressen der geschützten und getunnelten Knoten auf diesem Server. Der ViPNet Treiber auf dem DNS- bzw. WINS-Server (oder auf dem Coordinator, der diesen Server tunnelt) führt die Substitution der Adresse im IP-Paket durch die virtuelle oder reelle IP-Adresse durch.
- Bei Anfragen geschützter oder getunnelter Knoten an den DNS- und WINS-Server wird der Identifikator des angeforderten Knotens im ViPNet Netzwerk (oder der Identifikator des Coordinators, der diesen Knoten tunnelt) dem Antwortpaket hinzugefügt. Anhand dieses Identifikators ermittelt die ViPNet Software auf dem anfragenden Knoten (oder auf dem Coordinator, der diesen Knoten tunnelt) die korrekte Zugangsadresse zum angeforderten Knoten (ob reell oder virtuell).
- Wenn ein offener Computer Anfragen an den geschützten DNS- bzw. WINS-Server sendet, dann werden diese Anfragen von der ViPNet Software auf dem DNS- bzw. WINS-Server oder auf dem entsprechenden tunnelnden Coordinator so verarbeitet, dass dem offenen Computer die reellen IP-Adressen der geschützten und getunnelten Knoten mitgeteilt werden, auch dann, wenn für diese Knoten virtuelle IP-Adressen veröffentlicht sind.

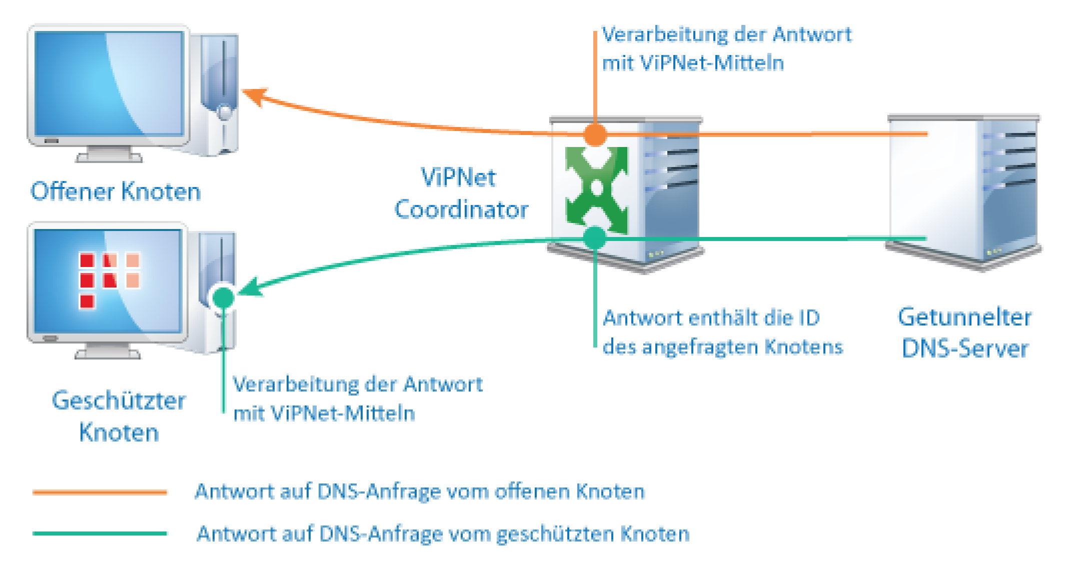


Abbildung 175. DNS-Server auf einem geschützten oder getunnelten Knoten

Konfigurationsempfehlungen

Bei Verwendung eines DNS- bzw. WINS-Servers, der sich auf einem geschützten oder getunnelten Knoten befindet, sollten Sie sich bei der Veröffentlichung virtueller IP-Adressen an folgende Empfehlungen halten:

- Beim manuellen Registrieren der IP-Adressen der geschützten und getunnelten Knoten auf dem DNS- bzw. WINS-Server sollten Sie die virtuellen oder reellen IP-Adressen dieser Knoten registrieren. Diese IP-Adressen sollten im Programm ViPNet Monitor auf dem DNS- bzw. WINS-Server oder auf dem Coordinator, der den Server tunnelt, sichtbar sein.
- Wenn sich der DNS- bzw. WINS-Server auf einem Knoten mit ViPNet Software befindet, dann dürfen im Subnetz dieses Servers keine Knoten untergebracht sein, die von irgendeinem Coordinator getunnelt werden und dabei Anfragen an den Server richten können (oder Gegenstand solcher Anfragen sein können). Wenn sich der Server auf dem Coordinator befindet, dann betrifft diese Anforderung die getunnelten Knoten anderer Coordinatoren.
- Wenn der DNS- bzw. WINS-Server vom Coordinator getunnelt wird, dann sollten im Subnetz dieses Servers keine Knoten mit installierter ViPNet Software untergebracht sein, die Anfragen an den Server richten können (oder Gegenstand solcher Anfragen sein können).
- Wenn die Notwendigkeit besteht, Knoten ungeachtet der aufgeführten Empfehlungen im Netzwerk unterzubringen, dann sollte auf den Knoten mit installierter ViPNet Software das Kontrollkästchen **Coordinator für die Tunnelung der lokalen IP-Adressen nicht verwenden** deaktiviert werden. Zusätzlich sollte auf den getunnelten Knoten eine gesonderte Route für die Weiterleitung des Traffics auf die Knoten mit ViPNet Software über den Coordinator konfiguriert werden.

Ungeschützter DNS- bzw. WINS-Server

Besonderheiten bei Verwendung

Es besteht häufig die Notwendigkeit, einen Zugang zum Coordinator zu erhalten, dessen externe Zugangsadresse auf der Seite der geschützten Knoten sich dynamisch ändern kann (Beispiel: der Coordinator ist über ein DSL-Modem mit dem Netzwerk verbunden). Die Aufgabe wird dadurch gelöst, dass diese Adresse auf dem öffentlichen DNS-Server im Internet veröffentlicht und der DNS-Name des Coordinators auf den anderen Netzwerkknoten im Programm ViPNet Monitor vorgegeben wird. In Firmennetzwerken kann es manchmal erforderlich sein, einen öffentlichen DNS-Server auch für andere Zwecke zu benutzen.

Öffentliche DNS-Server können jedoch häufig Ziel von unterschiedlichen Netzwerkangriffen sein, wobei die IP-Adresse des angefragten Netzwerkobjekts durch eine andere Adresse ersetzt wird mit dem Zweck, den geschützten Computer zum Verbindungsaufbau mit dem angreifenden Computer zu zwingen. Wenn ein solcher Angriff gelingt, wird der Netzwerkknoten beim Versuch, den Zugang zu einem geschützten Objekt über seinen DNS-Namen zu erhalten, eine offene Verbindung mit dem angreifenden Computer herstellen (da die IP-Adresse des angreifenden Computers dem ViPNet Treiber nicht bekannt ist). Dadurch bekommt der Angreifer die Möglichkeit, auf Daten auf dem geschützten Computer zuzugreifen.

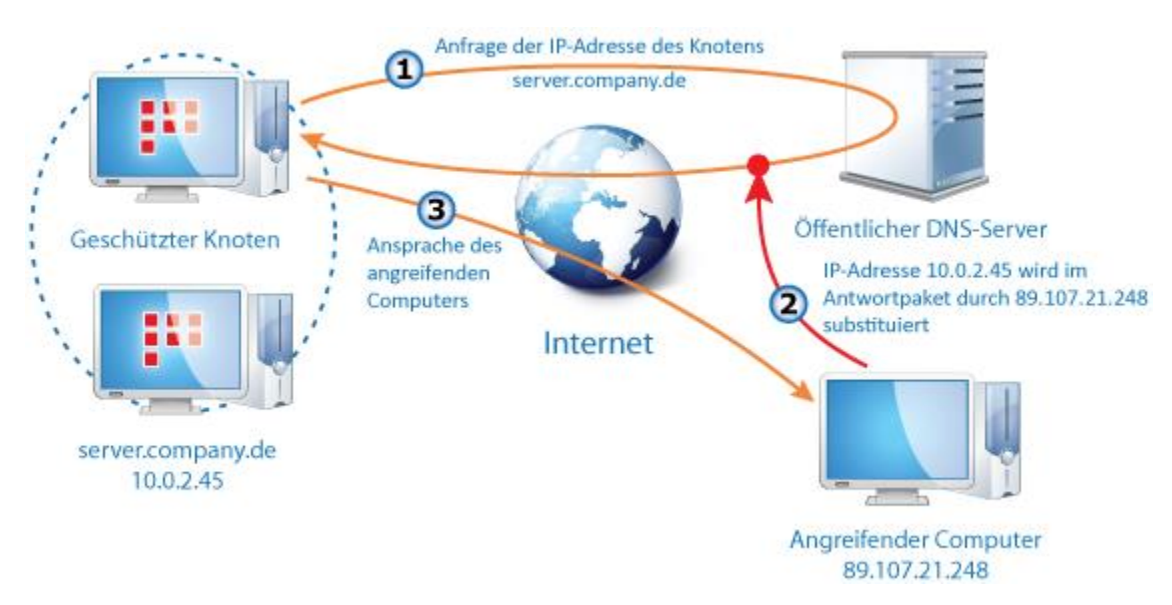


Abbildung 176. Angriff auf einen öffentlichen DNS-Server

Damit solche Angriffe verhindert werden, sollten für alle geschützten Anwendungsserver, die auf dem öffentlichen DNS-Server registriert und für andere geschützte Knoten zugänglich sind, die jeweiligen DNS-Namen im Programm ViPNet Monitor auf den geschützten Knoten angegeben werden. Bei einer Anfrage an den Server über seinen DNS-Namen wird dann, unabhängig von der IP-Adresse, die vom Angreifer vorgegeben wird, vom ViPNet Treiber beim Empfang der Anfrageantwort die ihm bereits

bekannte, sichtbare IP-Adresse des Knotens (reell oder virtuell) substituiert, die dem im Programm ViPNet Monitor angegebenen DNS-Namen entspricht.

Konfigurationsempfehlungen

Bei Verwendung eines offenen DNS-Servers sollten Sie sich an folgende Empfehlungen halten:

- Wenn sich die externe Zugangs-IP-Adresse des Coordinators ändern kann, und gleichzeitig der Zugang zu diesem Coordinator über seinen öffentlich registrierten DNS-Namen ermöglicht werden soll, dann sollte der DNS-Name des betroffenen Coordinators auf den geschützten Knoten im Programm ViPNet Monitor angegeben werden.
- Wenn ein Knoten mit installierter ViPNet Software auf andere geschützten Knoten über ihre virtuellen IP-Adressen zugreifen kann, und dabei der Zugang zu diesen Knoten über ihre öffentlich registrierten DNS-Namen ermöglicht werden soll, dann sollten diese DNS-Namen im Programm ViPNet Monitor angegeben werden. Auf dem offenen DNS-Server kann dabei eine beliebige IP-Adresse (reell oder virtuell) registriert sein. Die ViPNet Technologie gewährleistet den Aufbau von geschützten Verbindungen über die virtuelle sichtbare Adresse (s. Sichtbare Adressen auf S. 373) des Knotens unabhängig vom Typ der veröffentlichten IP-Adresse.
- Wie oben bereits erwähnt, sollten auch dann, wenn der Zugang zu geschützten Knoten über reelle IP-Adressen bereitgestellt wird, ihre DNS-Namen im Programm ViPNet Monitor angegeben werden, um die Sicherheit der Verbindung zu gewährleisten.

In allen beschriebenen Fällen können die DNS-Namen der geschützten Knoten manuell auf jedem einzelnen Netzwerkknoten angegeben werden. Es wird jedoch empfohlen, die DNS-Namen zentralisiert im Programm ViPNet Network Manager anzugeben.

Verwendung eines geschützten DNS- und WINS-Servers für Remote-Zugriff auf Unternehmensressourcen

Entfernte Benutzer können sich über das Internet mit dem ViPNet Netzwerk verbinden. Die Benutzer können zuhause, in einem Internet-Café, im Hotelzimmer oder an einem anderen Ort arbeiten, wobei die IP-Adressen und die genutzten DNS- und WINS-Server vom jeweiligen Internet-Provider bereitgestellt werden. Für die Arbeit mit vielen firmeninternen Anwendungen wird jedoch der DNS- oder WINS-Server des Firmennetzwerks benötigt. Durch die Verwendung eines firmeninternen DNS- und WINS-Servers können Remote-Benutzer auf die Server und andere Knoten des Firmennetzwerks nicht über deren IP-Adressen, sondern über ihre Namen zugreifen. Dabei wird die Umsetzung der DNS- und WINS-Namen in IP-Adressen sowohl für die Adressen des Firmennetzwerks als auch für die Adressen aus dem Internet durchgeführt.

Für den Remote-Zugriff auf firmeninterne Ressourcen sollten folgende Bedingungen erfüllt sein:

- Die Systemdatei hosts, welche die Zuordnung zwischen IP-Adressen und Computer-Namen festlegt, darf keine Einträge zu den Knoten des Firmennetzwerks enthalten. Diese Datei befindet sich im Ordner `%systemroot%\System32\drivers\etc\` (standardmäßig `C:\Windows\System32\drivers\etc\`).
- Im Programm ViPNet Monitor sollte der Zugang über eine Firewall mit dynamischem NAT eingestellt sein.
- In den Eigenschaften der Netzwerkverbindung sollte die Adresse des unternehmensinternen DNS(WINS)-Servers angegeben sein.

Sie können die Adresse des unternehmensinternen DNS-Servers in den Netzwerk-Verbindungseinstellungen manuell angeben. Es wird jedoch empfohlen, die Netzwerkknoten oder die getunnelten Objekte, auf denen sich die DNS-Server befinden, im Programm ViPNet Network Manager anzugeben. In diesem Fall wird die Liste der unternehmensinternen DNS-Server als Bestandteil von Schlüsseldistributionen an die ViPNet Netzwerkknoten weitergeleitet. Auf den Netzwerkknoten ermittelt das Programm ViPNet Monitor die aktuellen sichtbaren IP-Adressen der unternehmensinternen DNS-Server (reell oder virtuell) und ändert automatisch die Adressen der DNS-Server in den Netzwerkadaptereinstellungen des Computers.

Betrachten wir das folgende Beispiel. Ein Mitarbeiter, der in der Hauptniederlassung mit seinem Laptop und darauf installierter ViPNet Client-Software arbeitet, verbindet sich zum geschützten korporativen DNS-Server über eine bestimmte IP-Adresse (zum Beispiel 10.0.0.25). Zu einem gewissen Zeitpunkt besucht dieser Mitarbeiter mit seinem Laptop im Zuge einer Geschäftsreise eine andere Niederlassung. Dort ist der DNS-Server der Hauptniederlassung über eine andere IP-Adresse (zum Beispiel 11.0.0.3)

erreichbar. Der Mitarbeiter soll dabei in der Lage sein, über das Internet auf unternehmensinterne Ressourcen der Hauptniederlassung zuzugreifen.

Wenn der DNS-Server mit Hilfe des Betriebssystems registriert wurde, dann sind dazu Änderungen in den Netzwerk-Verbindungseinstellungen auf dem Laptop notwendig. Dies ist unbequem, da die Einstellungen bei der Rückkehr des Mitarbeiters in die Hauptniederlassung wieder zurückgesetzt werden müssen.



Komponenten von ViPNet Coordinator

ViPNet Programmkontrolle

Das Programm ViPNet Programmkontrolle ermöglicht die Überwachung von Netzwerkaktivitäten der auf dem Computer installierten Anwendungen. Folgende Netzwerkaktivitäten werden von ViPNet Programmkontrolle überwacht:

- Versuche, ausgehende Verbindungen herzustellen.
- Versuche, Ports für eingehende Verbindungen zu öffnen.
- Versenden von Datenpaketen ohne vorhergehenden Aufbau einer Verbindung.

Wählen Sie zum Starten des Programms ViPNet Programmkontrolle im Programm ViPNet Coordinator Monitor im Menü **Anwendungen** den Eintrag **Programmkontrolle**. Nunmehr wird das Programm ViPNet Programmkontrolle beim Start des Betriebssystems automatisch gestartet. ViPNet Programmkontrolle arbeitet unabhängig vom Programm ViPNet Monitor. Wenn ViPNet Monitor aus dem Arbeitsspeicher des Computers entladen wird, setzt das Programm ViPNet Programmkontrolle seine Arbeit fort, bis es vom Benutzer beendet wird.



Hinweis. Das vorliegende Kapitel beinhaltet eine kurze Beschreibung des Programms ViPNet Programmkontrolle. Ausführliche Informationen sind in der Programm-Hilfe enthalten (Aufruf durch Drücken der **F1**-Taste oder über das Menü **Hilfe**).

Funktionsweise von ViPNet Programmkontrolle

Aus der Sicht von ViPNet Programmkontrolle werden alle Programme, die versuchen, einen Netzwerkzugang zu erhalten, in zwei Typen unterteilt:

- Windows-Dienste. Das sind Spezialprogramme, die unter Windows unterschiedliche Funktionen ausführen. Als Beispiele für Windows-Dienste können der Windows-Zeitgeber, der DNS-Client, der Web-Publishingdienst (Web-Server) und andere client- oder serverseitige Anwendungen angeführt werden. Diese Anwendungen können sowohl lokale wie auch Netzwerk-Benutzer unterstützen. Windows-Dienste arbeiten häufig im Hintergrund und besitzen viele Gemeinsamkeiten mit UNIX-Daemons. Einige Anwendungen verfügen über eine ausführbare Programmdatei, starten aber mehrere Dienste.
- Andere Anwendungen wie zum Beispiel MS Internet Explorer oder weitere von Ihnen installierte Programme (von Skype bis World of Warcraft).

Sobald irgendeine Anwendung versucht, auf das Netzwerk zuzugreifen, wird ihre Arbeit im Netzwerk von ViPNet Programmkontrolle in Abhängigkeit von den aktuellen Einstellungen entweder erlaubt oder blockiert, oder es wird eine Meldung ausgegeben.

Beim erstmaligen Feststellen von Netzwerkaktivitäten irgendeiner Anwendung wird der Netzwerkzugang dieser Anwendung vom Programm ViPNet Programmkontrolle standardmäßig erlaubt. Zusätzlich wird ein

Meldungsfenster eingeblendet, in dem ausgewählt werden kann, welche Aktionen bei nachfolgenden Netzwerkaktivitäten der gegebenen Anwendung durchgeführt werden sollen.

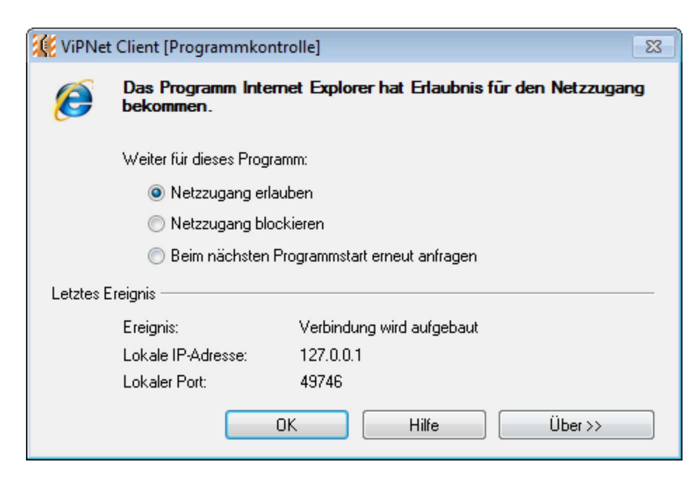


Abbildung 177. Meldung über Netzwerkaktivität einer Anwendung

Im Meldungsfenster werden außerdem Informationen über die betroffene Anwendung sowie über das letzte Ereignis, das von ViPNet Programmkontrolle registriert wurde, angezeigt: Ereignistyp, IP-Adresse, die für den Zugriffsversuch verwendet wurde, und Portnummer (soweit vorhanden).

Beim Erhalt einer solchen Meldung:

1. Wählen Sie eine Aktion aus, die im Hinblick auf die gegebene Anwendung beim nächsten Versuch eines Netzzugriffs ausgeführt werden soll. Unter Verwendung von Standardeinstellungen stehen folgende Optionen zur Verfügung:
   - **Netzzugang erlauben**: Anwendung zur Liste **Registrierte Anwendungen** (s. Registrierung der Anwendungen auf S. 316) hinzufügen und den Netzzugang dieser Anwendung beim nächsten Zugriffsversuch erlauben.
   - **Netzzugang blockieren**: Anwendung zur Liste **Registrierte Anwendungen** hinzufügen und den Netzzugang dieser Anwendung beim nächsten Zugriffsversuch blockieren.
   - **Beim nächsten Programmstart erneut anfragen**: Anwendung nicht zur Liste **Registrierte Anwendungen** hinzufügen und beim nächsten Zugriffsversuch die Aktion ausführen, die in den aktuellen Einstellungen von ViPNet Programmkontrolle festgelegt ist.
2. Klicken Sie zum Anzeigen zusätzlicher Informationen über das Programm auf die Schaltfläche **Über**. Unter der Überschrift **Über das Programm** werden der Name des Programms, der Hersteller, die Version und der Pfad zur ausführbaren Programmdatei aufgelistet.

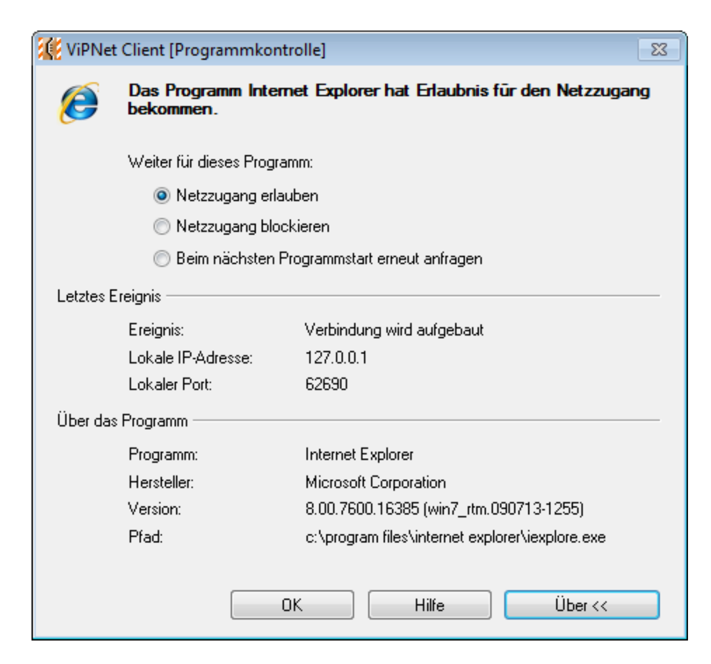


Abbildung 178. Zusätzliche Informationen über die Anwendung anzeigen

3 Nachdem Sie eine Aktion für das betroffene Programm ausgewählt haben, klicken Sie auf **OK**.



Achtung! Wenn ViPNet Programmkontrolle den Dateipfad der Anwendung, die versucht, auf das Netzwerk zuzugreifen, nicht festlegen kann, wird der Netzzugang für diese Anwendung temporär erlaubt. Das Programm wird im Netzwerk arbeiten können, bis ViPNet Programmkontrolle beendet wird. Das Programm wird aber nicht in die Liste **Registrierte Anwendungen** eingetragen, und in der Logdatei von ViPNet Programmkontrolle wird kein entsprechender Ereigniseintrag erstellt.

Wenn sich die Datei einer in der Liste **Registrierte Anwendungen** eingetragenen Anwendung ändert, dann wird von ViPNet Programmkontrolle eine entsprechende Meldung ausgegeben. Im Meldungsfenster können Sie den Netzzugang dieses Programms erlauben oder blockieren, oder die Entscheidung darüber bis zum nächsten Zugriffsversuch verschieben (die Standardaktion kann im Bereich **Einstellungen** konfiguriert werden).

Registrierung der Anwendungen

Sie können Anwendungen selbständig in der Liste der **Registrierten Anwendungen** hinzufügen, um ihnen den Zugang zum Netzwerk zu erlauben oder zu blockieren.

Führen Sie zum Ändern der Liste der registrierten Anwendungen die folgenden Schritte aus:

1 Zum Registrieren einer Anwendung:

1.1 Wählen Sie im Hauptfenster von ViPNet Programmkontrolle im Menü **Optionen** den Eintrag **Programm konfigurieren**.

1.2 Klicken Sie im Untermenü auf den Eintrag **Netzzugang erlauben** oder **Netzzugang blockieren**.

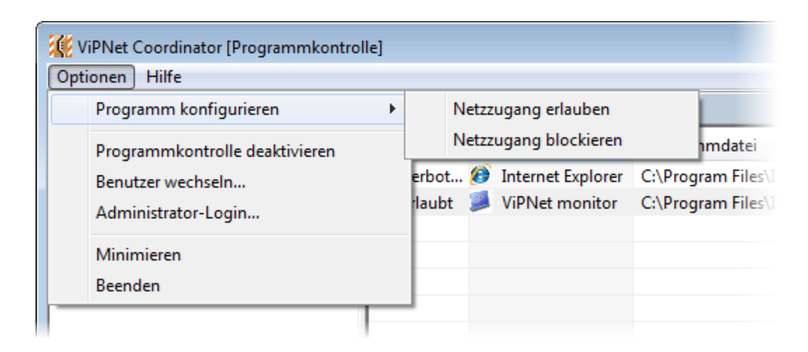


Abbildung 179. Anwendung mit erlaubtem Netzzugang registrieren

1.3 Geben Sie im Fenster **Programm zur Liste hinzufügen** den Pfad zur ausführbaren Programmdatei an, für die der Netzzugang erlaubt oder blockiert werden soll, und klicken auf die Schaltfläche **Öffnen**.

Das gewählte Programm wird in der Liste **Registrierte Anwendungen** hinzugefügt.

2 Wenn Sie den Netzwerk-Zugriffserlaubnis für eine Anwendung ändern möchten, dann klicken Sie mit der rechten Maustaste auf die Anwendung und wählen im Kontextmenü **Netzzugang blockieren** oder **Netzzugang erlauben**.

3 Wenn Sie eine Anwendung aus der Liste löschen möchten, wählen Sie diese Anwendung aus und drücken die **Entf**-Taste.

Transportmodul ViPNet MFTP

Das Transportmodul MFTP ist eine wichtige Komponente von ViPNet Client und ViPNet Coordinator. Dieses Modul sorgt für die Übertragung von Transportdateien (s. Datei (Transportdatei) auf S. 370), die Daten der Anwendungen ViPNet Business Mail und FileExchange sowie Dienstinformationen des Programms ViPNet Network Manager enthalten, zwischen den einzelnen ViPNet Netzwerkknoten.

Auf dem Coordinator arbeitet das MFTP-Modul im sogenannten Server-Modus. Es wird gemeinsam mit dem Programm ViPNet Monitor gestartet und bleibt während der gesamten Laufzeit des Programms aktiv. Beim Erhalt von Transportdateien bestimmt das MFTP-Modul die weitere Route für die Übertragung und leitet die Dateien an den nächsten Netzwerkknoten weiter. Wenn die Datei über mehrere Adressaten verfügt, wird sie in Übereinstimmung mit der Empfängerliste versendet. Abhängig von den gesetzten Parametern initiiert entweder das MFTP-Modul des Coordinators die Verbindung für die Weiterleitung der Datei an den Empfänger oder es wartet auf den planmäßigen Verbindungsaufbau seitens des Empfänger-Moduls.



Hinweis. Wenn während der Weiterleitung einer Datei die Verbindung zwischen dem Sender- und dem Empfänger-MFTP-Modul unterbrochen wird, dann wird nach dem Wiederherstellen der Verbindung die Fortsetzung der Weiterleitung der Datei ab dem Zeitpunkt der Unterbrechung fortgesetzt. Diese Eigenschaft wird in der Terminologie der FTP-Clients als „Möglichkeit zur Fortsetzung des Up-/Downloads“ bezeichnet.

Das MFTP-Modul des Clients verbindet sich regelmäßig mit dem Kommunikationsserver (Coordinator, auf dem der Client in ViPNet Network Manager registriert ist) und fordert Transportdateien an, die für den betreffenden Client bestimmt sind. Sind solche Dateien vorhanden, werden sie vom Modul nach einer vorangehenden beidseitigen Authentifizierung geladen. Nach dem Laden der letzten verfügbaren Datei stellt das Modul die Arbeit ein, und wird nach 15 Minuten neu gestartet, um die nächste Ladung verfügbarer Dateien anzufordern (dieses Intervall ist standardmäßig voreingestellt und kann geändert werden). Dieser Arbeitsmodus des MFTP-Moduls wird als Client-Modus bezeichnet. Wenn die Anwendung ViPNet Business Mail gestartet ist, bleibt das MFTP-Modul aktiv bis eine Abmeldung in Business Mail erfolgt. Wenn mit Hilfe von FileExchange Dateien oder Ordner versendet werden, wird das MFTP-Modul für die Durchführung dieser Aufgabe gestartet und nach dem Beenden der Arbeit aus dem Hauptspeicher entladen.



Hinweis. Das vorliegende Kapitel beinhaltet eine kurze Beschreibung des MFTP-Transportmoduls. Ausführliche Informationen sind in der Programm-Hilfe enthalten (Aufruf der Hilfe durch Drücken der **F1**-Taste oder über das Menü **Hilfe**).

Suchen von Dateien in Warteschlange und Übermittlungsprotokoll

Wählen Sie zum Aufrufen des Programmfensters des MFTP-Moduls im Hauptfenster von ViPNet Monitor im Menü **Anwendungen** den Befehl **Transportmodul**.

Im oberen Fensterteil werden vier Statusanzeigen für die Abbildung des Fortschritts beim Senden und Empfangen von Dateien angezeigt.



Hinweis. Die vier Statusanzeigen erlauben eine gleichzeitige Überwachung des Sende- und Empfangvorgangs von vier Dateien. Solche Situationen können auf Coordinatoren häufig auftreten.

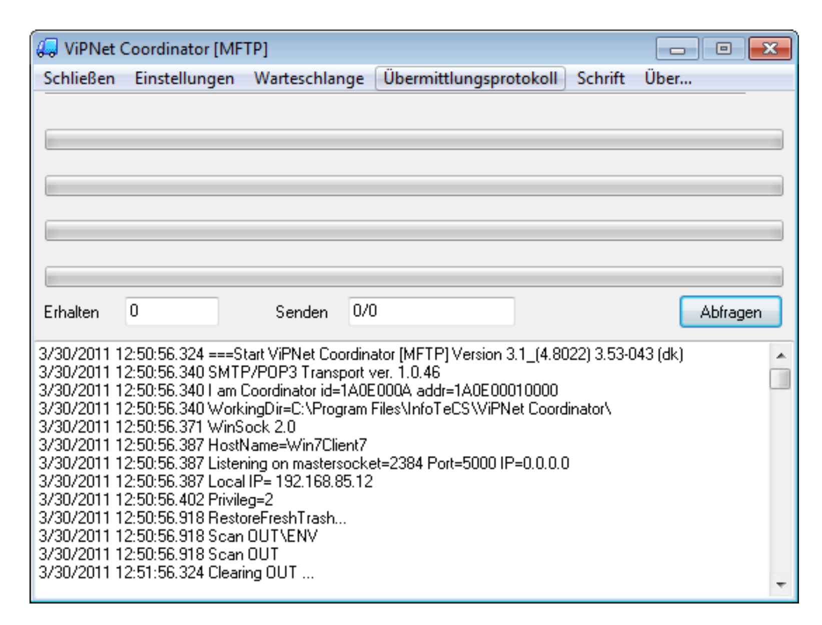


Abbildung 180. Programmfenster des MFTP-Moduls

Im unteren Fensterteil werden Informationen über hergestellte und unterbrochene Verbindungen ausgegeben. Diese Informationen können bei der Durchführung technischer Wartungsarbeiten hilfreich sein, haben aber keinen Wert für den Benutzer. Standardmäßig werden die Daten der letzten 10 Tage angezeigt.

Klicken Sie auf die Schaltfläche **Abfragen**, damit sich das MFTP-Modul sofort mit dem Coordinator (und mit anderen Netzwerkknoten, mit denen ein direkter Datenaustausch mit Hilfe des MFTP-Moduls durchgeführt wird) verbindet.

Klicken Sie im Menü **Schließen** auf **Verstecken**, um das Programmfenster des MFTP-Moduls zu minimieren. Sie können auch die **Esc**-Taste drücken.

Wählen Sie zum Beenden der Arbeit im MFTP-Modul im Menü **Schließen** den Punkt **Beenden** oder drücken die Tastenkombination **Alt+F4**.



Achtung! Es wird nicht empfohlen, die Parameter des MFTP-Moduls über den Menüpunkt **Einstellungen** zu ändern. Die Konfiguration des Transportmoduls sollte nur in besonderen Fällen von qualifizierten Administratoren des ViPNet Netzwerks durchgeführt werden. Wenn Änderungen an der Konfiguration des MFTP-Moduls unbedingt erforderlich sind, wenden Sie sich an den Kundendienst von Infotecs GmbH.

Suchen von Dateien in der Warteschlange

Dateien, die noch nicht an ihre Empfänger versendet wurden (wegen fehlender Verbindung oder wegen des Versands anderer Dateien zum gegebenen Zeitpunkt), werden in der Datei-Warteschlange gesammelt. Zum Suchen von Dateien in der Warteschlange:

1 Klicken Sie im Hauptmenü des MFTP-Moduls auf **Warteschlange**.

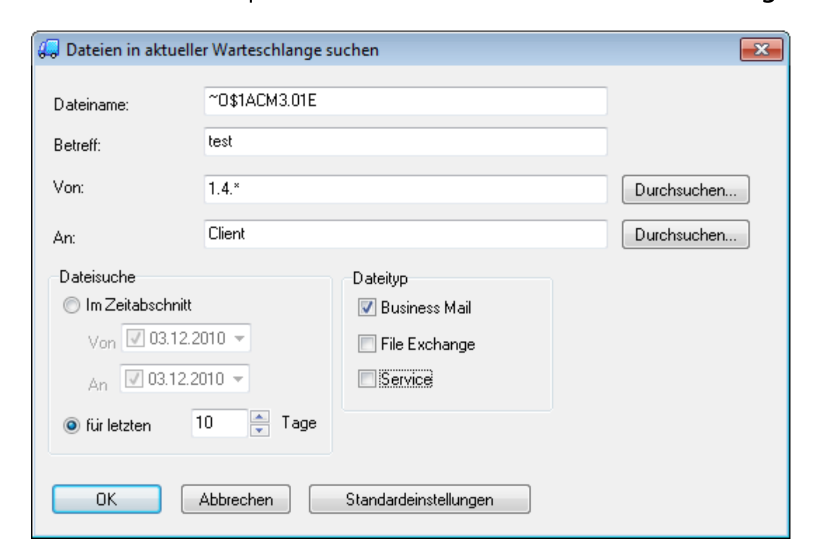


Abbildung 181. Dateien in Warteschlange suchen

2 Geben Sie im Fenster **Dateien in aktueller Warteschlange suchen** die Suchparameter an und klicken auf **OK**. Es wird eine Liste von Dateien angezeigt, die den Suchparametern entsprechen.

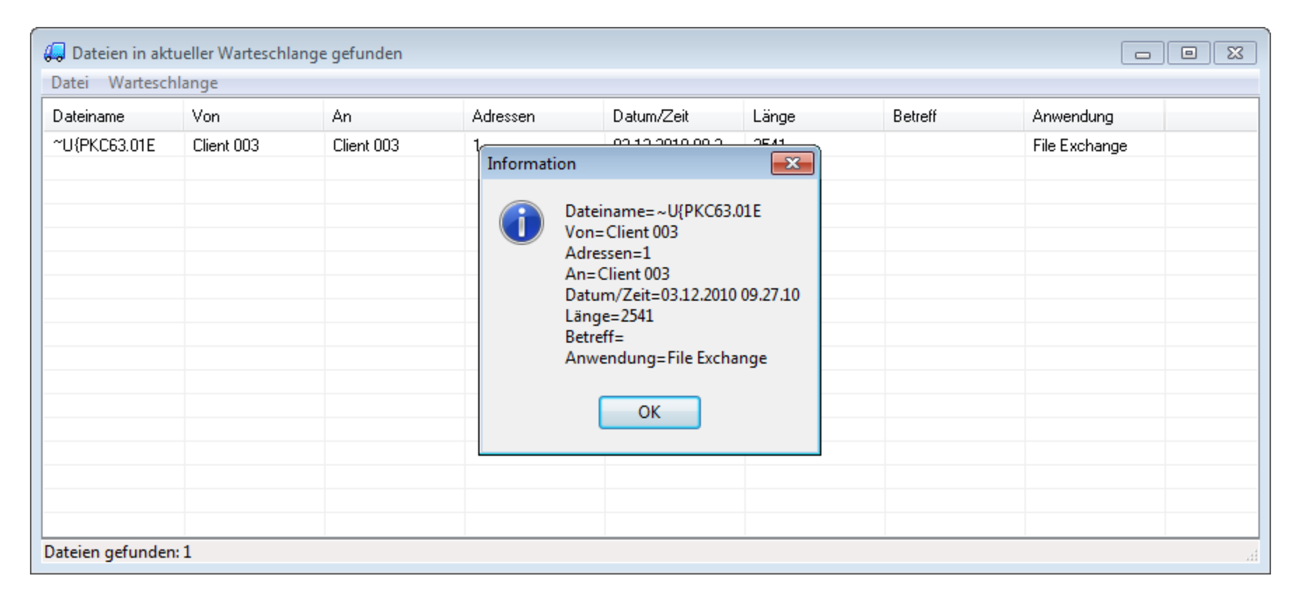


Abbildung 182. Ergebnisse der Suche in der Warteschlange

3 Im Fenster **Dateien in aktueller Warteschlange gefunden** sind folgende Aktionen möglich:

- Wenn Sie Detailinformationen über eine nicht versendete Datei anzeigen möchten, wählen Sie diese Datei in der Liste aus und klicken im Menü **Datei** auf den Eintrag **Eigenschaften**.
- Wenn Sie eine Datei in einen Ordner auf der Festplatte kopieren oder verschieben möchten (um die Datei zum Beispiel manuell weiterzuleiten), dann wählen Sie diese Datei aus und klicken im Menü **Datei** auf **Kopieren** (oder **Verschieben**).
- Wenn Sie eine nicht versendete Datei aus der Warteschlange entfernen möchten, wählen Sie diese Datei in der Liste aus und drücken die **Entf**-Taste.
- Wenn Sie die Suchergebnisse im Web-Browser oder in Microsoft Excel anzeigen oder in einer Datei speichern möchten, klicken Sie im Menü **Warteschlange** auf einen der Punkte: **In HTML-Format anzeigen**, **Als Excel-Tabelle anzeigen**, **Speichern als**.



Tipp. Um die Vertraulichkeit der Daten sicherzustellen, kann die Funktion für das sichere Entfernen von Dateien aus der Warteschlange benutzt werden (Menü **Datei** > **Sicher löschen**). Dateien, die mit Hilfe dieser Funktion gelöscht wurden, können nicht wiederhergestellt werden.

Suchen von Dateien im Übermittlungsprotokoll

Zum Suchen von beliebigen gesendeten oder empfangenen Dateien:

1 Klicken Sie im Hauptmenü des MFTP-Moduls auf **Übermittlungsprotokoll**.

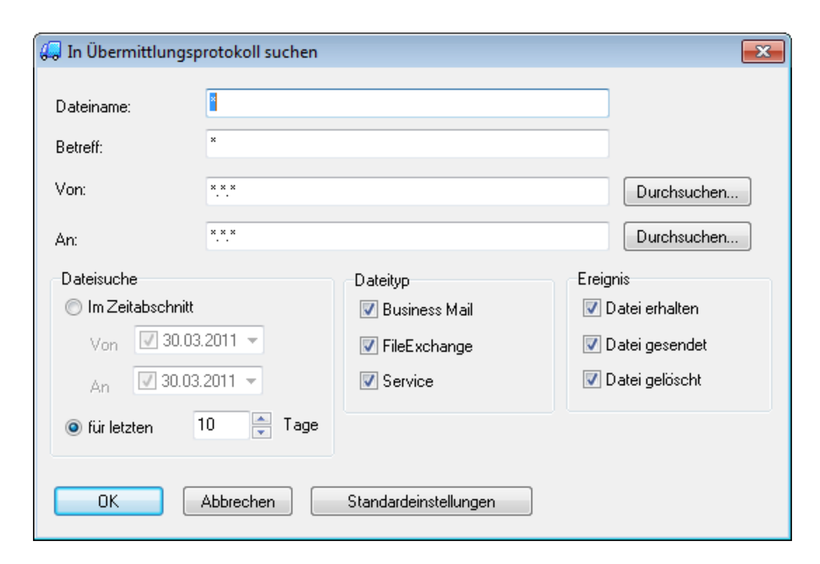


Abbildung 183. Dateien im Übermittlungsprotokoll suchen

2 Geben Sie im Fenster **In Übermittlungsprotokoll suchen** die Suchparameter an und klicken auf **OK**. Es wird eine Liste von Dateien eingeblendet, die den Suchparametern entsprechen.

3 Im Fenster **Dateien in Übermittlungsprotokoll gefunden** sind die folgende Aktionen möglich:

- Wenn Sie Detailinformationen über eine nicht versendete Datei anzeigen möchten, wählen Sie diese Datei in der Liste aus und klicken im Menü **Datei** auf **Eigenschaften**.
- Wenn Sie die Suchergebnisse im Web-Browser oder in Microsoft Excel anzeigen oder in einer Datei speichern möchten, klicken Sie im Menü **Übermittlungsprotokoll** auf einen der Punkte: **In HTML-Format anzeigen**, **Als Excel-Tabelle anzeigen**, **Speichern als**.

18

Administrative Funktionen von ViPNet Monitor



Hinweis. Die Informationen in diesem Kapitel beziehen sich sowohl auf ViPNet Coordinator als auch auf ViPNet Client.

Verwendung der Logdatei

Im Bereich **Logdatei** können die Benutzer auf Basis unterschiedlicher Suchoptionen Berichte über IP-Pakete erstellen, die im Programm registriert wurden. Diese Berichte ermöglichen eine Kontrolle der ein- und ausgehenden Verbindungen des Computers.

Anzeige der Suchergebnisse

Nach dem Klicken auf die Schaltfläche **Suche** wird die Suche entsprechend der im Bereich **Erweiterte Suchoptionen** eingestellten Parameter durchgeführt. Die Suchergebnisse werden im Fenster **Logdatei** angezeigt.

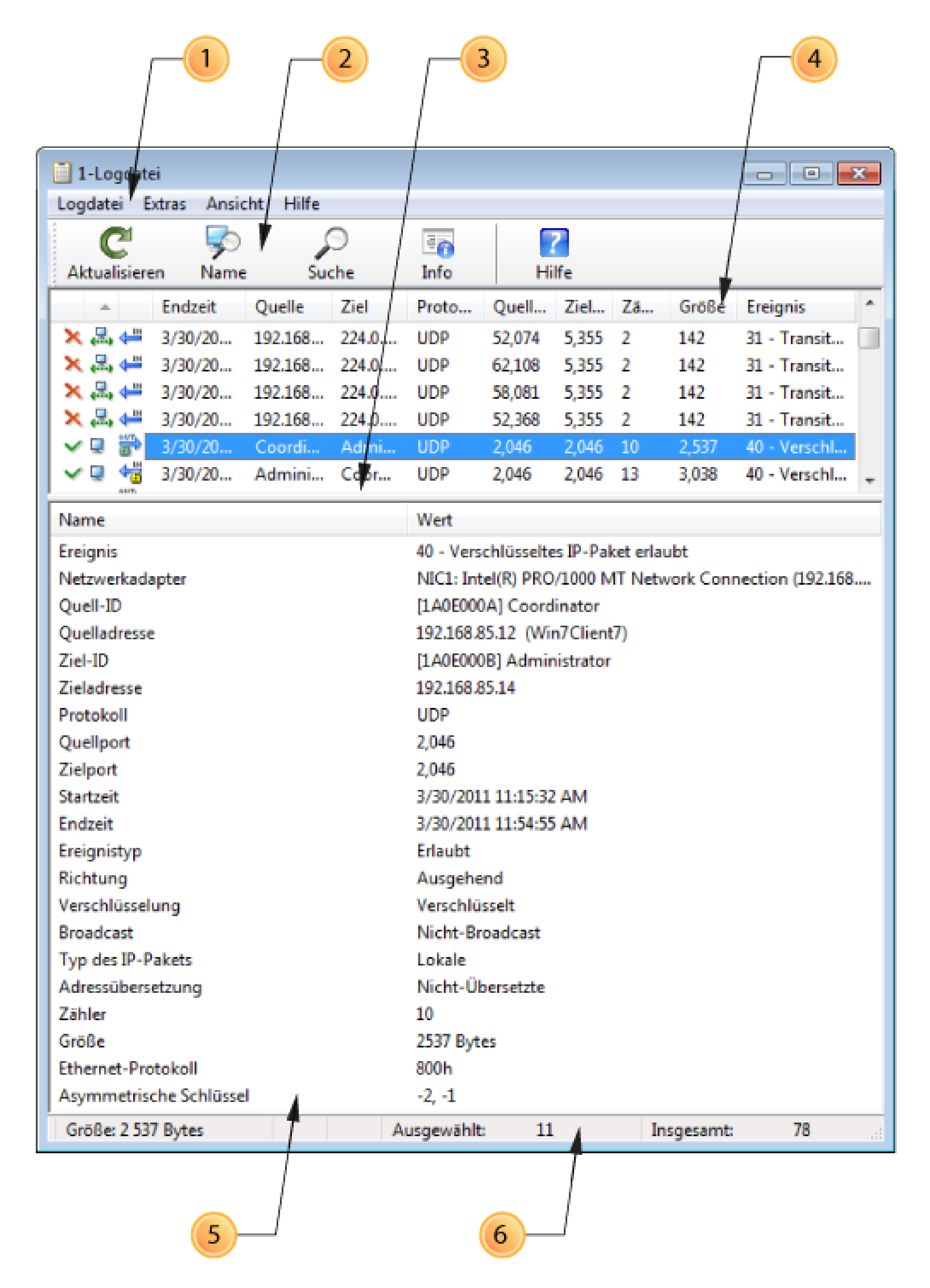


Abbildung 184. Anzeige der Logdatei der IP-Pakete (Coordinator)

Mit den Zahlen 1 bis 6 sind in der oberen Abbildung folgende Elemente gekennzeichnet:

1 Das Hauptmenü.

2 Die Symbolleiste. Wählen Sie im Menü **Ansicht** die Option **Symbolleiste anpassen** aus, um eine Schaltfläche von der Symbolleiste zu löschen oder in die Leiste einzufügen.

3 Der Hauptbereich enthält eine Liste der Logdatei-Einträge, die den definierten Suchoptionen entsprechen.

- Wenn Sie Informationen über ein ausgewähltes Paket in einem neuen Fenster anzeigen möchten, klicken Sie auf die Schaltfläche **Info** in der Symbolleiste des Fensters **Logdatei**.
- Wenn Sie den Sender- oder Empfängernamen eines bestimmten Pakets festlegen möchten, klicken Sie auf die Schaltfläche **Name** in der Symbolleiste oder klicken mit der rechten Maustaste auf den entsprechenden Eintrag und wählen im Kontextmenü den Befehl **Computername auflösen**.

4 Die Spalten des Hauptbereichs.

5 Der Bereich der Paketeigenschaften enthält ausführliche Informationen über das im Hauptbereich ausgewählte Paket (**3**).

6 Die Statusleiste enthält die Größe des ausgewählten Pakets (bzw. der Paketgruppe) in Bytes, die aktuelle Eintragsnummer und die Gesamtanzahl der gefundenen Einträge. Wenn im Hauptbereich (**3**) mehrere Pakete ausgewählt sind, wird in der Statusleiste das Gesamtgröße dieser Pakete angezeigt.

Empfehlungen zur Analyse offener (nicht verschlüsselter) und verschlüsselter Verbindungen

Für eine bequemere Analyse aller offenen Verbindungen in der Logdatei werden folgende Einstellungen empfohlen:

1 Klicken Sie im Fenster **Logdatei** mit der rechten Maustaste auf eine beliebige Spaltenüberschrift.

2 Wählen Sie **Spalten hinzufügen** im eingeblendeten Kontextmenü.

3 Zum Analysieren:

- der offenen (nicht verschlüsselten) Verbindungen:
    - Stellen Sie im Fenster **Spalten anpassen** die Anzeige der folgenden Spalten ein: **Quelladresse**, **Zieladresse**.
    - Stellen Sie im Fenster **Spalten anpassen** die Anzeige der folgenden Spalten ein: **Quelle**, **Quell-ID**, **Ziel**, **Ziel-ID**.
- der verschlüsselten Verbindungen:
    - Stellen Sie im Fenster **Spalten anpassen** die Anzeige der folgenden Spalten ein: **Quelle-ID**, **Ziel-ID**.
    - Stellen Sie im Fenster **Spalten anpassen** die Anzeige für folgende Spalten ein: **Quelladresse**, **Zieladresse**.

4 Nachdem Sie die Konfiguration der Einstellungen abgeschlossen haben, klicken Sie auf die Schaltfläche **OK** um das Fenster zu schließen und die Änderungen zu speichern oder klicken auf die Schaltfläche **Abbrechen**, um die vorgenommenen Einstellungen nicht zu übernehmen.

Anzeige der Logdateien anderer Netzwerkknoten

Beim Arbeiten im Administratormodus ist es möglich, die Logdatei der IP-Pakete eines anderen ViPNet Netzwerkknoten, der mit dem gegebenen Netzwerkknoten verbundenen ist, anzuzeigen. Gehen Sie dazu wie folgt vor:

1. Melden Sie sich im Programm im Administratormodus an (s. Arbeiten mit Administratorrechten auf S. 338).
2. Wählen Sie im Programmfenster von ViPNet Monitor in der Navigationsleiste den Bereich **Logdatei**.
3. Wählen Sie in der Liste **Netzwerkknoten** den Netzwerkknoten aus, dessen Logdatei angezeigt werden soll. Wenn der Netzwerkknoten nicht in der Liste enthalten ist, klicken Sie auf die Schaltfläche ... und legen den benötigten Knoten im Fenster **ViPNet Knoten auswählen** fest.
4. Nachdem der benötigte Netzwerkknoten ausgewählt wurde, wird eine Verbindung mit diesem Knoten hergestellt. Sobald die Verbindung erfolgreich hergestellt werden konnte, wird der Name des gesuchten Netzwerkknotens in der Liste **Netzwerkknoten** angezeigt. Um den Verbindungsvorgang abzubrechen, klicken Sie auf die Schaltfläche **Abbrechen**.



Hinweis. Wenn auf dem Netzwerkknoten, dessen Logdatei angefragt wird, die Version der installierten ViPNet Software niedriger als 3.0 ist, werden die Suchparameter wesentlich eingeschränkt. Dies liegt daran, dass das Format der Logdatei der IP-Pakete in Version 3.0 geändert wurde. Bei Einschränkung der Suchoptionen wird eine entsprechende Meldung angezeigt.

Es sollte beachtet werden, dass die Suchparameter beim Anzeigen der Logdatei eines anderen Netzwerkknotens an den Typ dieses Knotens angepasst werden. Wenn also im Programm ViPNet Coordinator die Logdatei eines Clients angefragt wird, können nur die für einen Client verfügbaren Parameter angegeben werden.

5. Geben Sie die Suchparameter an und klicken auf die Schaltfläche **Suche**.

Einstellen der Suchoptionen

Zum Anzeigen der Logdatei der IP-Pakete:

1. Wählen Sie im Programmfenster von ViPNet Monitor in der Navigationsleiste den Bereich **Logdatei**.
2. Geben Sie im Bereich **Erweiterte Suchoptionen** Sie die Zeit der Registrierung des IP-Pakets, die gewünschte Anzahl der Einträge und auch folgende Suchoptionen:
   - Wenn Sie IP-Pakete im Programm ViPNet Coordinator suchen, wählen Sie in der Liste **Netzwerkadapter** den Netzwerkadapter des Coordinators aus, über den die gesuchten IP-Pakete übertragen wurden.
   - Wählen Sie in der Liste **Typ des Datenverkehrs** den Traffic-Typ, zu denen die IP-Pakete gehören.

- Wählen Sie in der Liste **Ereignis** einen bestimmten Ereignistyp oder eine Gruppe von Ereignistypen aus, die ViPNet Monitor jedem IP-Paket zuordnet. Eine Beschreibung der Ereignistypen finden Sie in der Kontexthilfe des Programms ViPNet Monitor.
- Geben Sie in Gruppe **Eigener Netzwerkknoten** (für Clients) oder **Netzwerkknoten <1>** (für Coordinatoren) die IP-Adresse oder den Namen des ViPNet Netzwerkknotens an, der als einer der Verbindungsteilnehmer (Empfänger oder Absender der IP-Pakete) auftritt.
- Geben Sie in Gruppe **Externer Netzwerkknoten** (für Clients) oder **Netzwerkknoten <2>** (für Coordinatoren) die IP-Adresse oder den Namen des ViPNet Netzwerkknotens, der als zweiter Verbindungsteilnehmer (Absender oder Empfänger der IP-Pakete) auftritt.
- Wählen Sie in der Liste **Protokoll** das Übertragungsprotokoll der gesuchten IP-Pakete aus. Falls das nötige Protokoll in der Liste nicht vorhanden ist, klicken Sie auf die Schaltfläche und fügen das Protokoll im Fenster **Protokollliste** hinzu.
- Wählen Sie in Gruppe **Eigenschaften der IP-Pakete** die Übertragungsrichtung der gesuchten IP-Pakete (die Liste **Richtung**), den Typ der IP-Pakete (die Liste **Broadcast** und **NAT**) und der Quelle der IP-Pakete (Liste **Absender**) aus.
- Wenn Sie die Standardsuchparameter wiederherstellen möchten, klicken Sie auf die Schaltfläche **Standardparameter**.

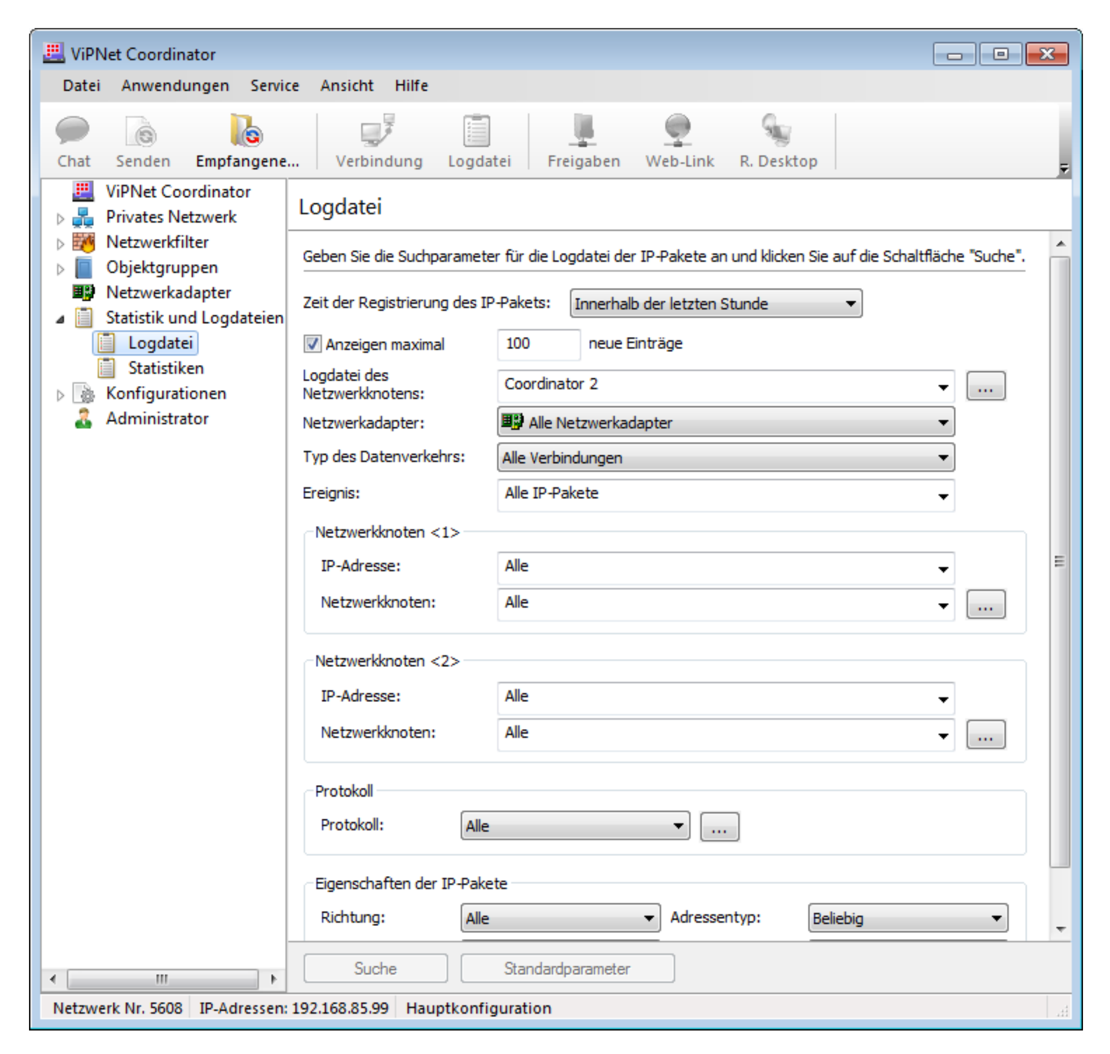


Abbildung 185. Einstellung der Suchoptionen für die Logdatei

3 Nachdem Sie alle Suchoptionen eingegeben haben, klicken Sie auf die Schaltfläche **Suche**.



Hinweis. Wenn Sie eine Suche mit Hilfe der Standardoptionen durchführen, dann werden im Bericht maximal 100 Einträge über IP-Pakete, die innerhalb der letzten Stunde registriert wurden, angezeigt.

Anzeige der archivierten Logdateien

Die Archivierung der Logdateien wird dazu verwendet, die Suche nach IP-Paketen zu optimieren und den Speicherplatz auf der Festplatte effektiver zu nutzen.

Ein neues Archiv wird dann erstellt, wenn die aktuelle Logdatei die maximal zulässige Größe erreicht hat. Dieser Wert wird durch den Parameter **Maximale Größe der Logdatei** bestimmt. Wenn der Parameter auf der Wert `0` eingestellt ist, findet keine Archivierung statt.

Zum Anzeigen der archivierten Logdatei der IP-Pakete:

1 Wählen Sie im Programmfenster von ViPNet Monitor im Bereich **Logdatei** den Unterbereich **Archiv** und klicken dann auf das Archiv mit dem benötigten Zeitintervall.



Hinweis. Wenn der Bereich **Archiv** nicht angezeigt wird, dann bedeutet das, dass vom System bislang noch kein Archiv erstellt wurde.

2 Geben Sie die Parameter für die Suche im Logdatei-Archiv an.

3 Die Suchergebnisse werden im Fenster **Logdatei** angezeigt.



Tipp. Wenn Sie alte Logdatei-Archive löschen möchten, wählen Sie im Unterbereich **Archiv** eines oder mehrere Archive aus und drücken die Taste **Entf** oder benutzen den Befehl **Löschen** im Kontextmenü.

Steuerung von Programmkonfigurationen

Eine Konfiguration stellt die Gesamtheit aller Einstellungen des Programms ViPNet Monitor dar. Im Bereich **Konfigurationen** können zusätzliche Konfigurationen erstellt und eine bestimmte Konfiguration jederzeit als aktive Konfiguration festgelegt werden.

Die Verwendung mehrerer Konfigurationen kann dann nützlich sein, wenn die korporative Sicherheitsrichtlinie den gleichzeitigen Zugriff auf lokale und Internet-Ressourcen untersagt. In diesem Fall sollten zwei Konfigurationen erstellt werden: in der ersten Konfiguration sollten die Arbeit im Internet erlaubt und der Zugang zum lokalen Netzwerk blockiert sein, in der zweiten Konfiguration sollten die Arbeit im lokalen Netzwerk erlaubt und der Zugang zum Internet blockiert sein. Oder es müssen z. B. die Verbindungseinstellungen für das private Netzwerk regelmäßig geändert werden. Aus praktischen Gründen können Sie in diesem Fall mehrere Konfigurationen mit unterschiedlichen Verbindungseinstellungen für das private Netzwerk definieren. In der Folge müssen die Einstellungen nicht jedes Mal geändert werden. Es genügt, eine Konfiguration mit passenden Einstellungen auszuwählen.

Beim ersten Start des Programms wird die **Hauptkonfiguration** erstellt, die Standardeinstellungen enthält. Diese Konfiguration kann nicht umbenannt oder gelöscht werden.

Verwendung der ViPNet Client-Konfigurationen ist nur im Administratormodus möglich.

Wenn Sie eine neue Konfiguration von ViPNet Monitor erstellen möchten:

1 Klicken Sie im Programmfenster von ViPNet Monitor in der Navigationsleiste mit der rechten Maustaste auf den Bereich **Konfigurationen** und wählen im Kontextmenü den Befehl **Neue Konfiguration erstellen**.

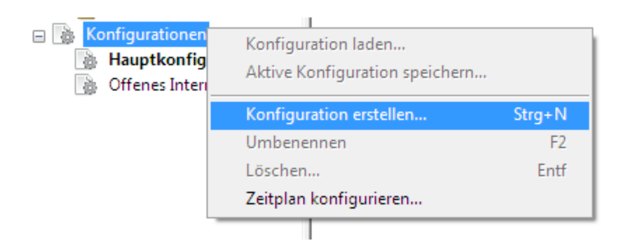


Abbildung 186. Erstellung einer neuen Konfiguration

In der Liste der Konfigurationen wird der Eintrag **Neue Konfiguration** angezeigt.



Hinweis. Im Administratormodus können Programmkonfigurationen für jeden beliebigen Benutzer erstellt werden, der auf dem Knoten registriert ist. In diesem Modus werden alle Konfigurationen angezeigt, die während der Arbeit mit dem Programm angelegt wurden. Die Konfigurationen werden dabei nach dem Benutzer, in dessen Namen sie erstellt wurden, gruppiert.

2 Klicken Sie auf die Konfiguration mit der rechten Maustaste und wählen im Kontextmenü den Befehl **Umbenennen**, um dieser Konfiguration einen neuen Namen zuzuweisen.

3 Klicken Sie zum Laden (Aktivieren) einer vorhandenen Konfigurationen mit der rechten Maustaste auf die benötigte Konfiguration und wählen im Kontextmenü den Befehl **Aktuelle Konfiguration festlegen**.



Hinweis. Sie können die benötigte Konfiguration auch über das Hauptmenü des Programms **Datei** > **Konfigurationen** oder aus dem Kontextmenü des Programmsymbols von ViPNet Monitor im Infobereich der Taskleiste laden.

4 Wenn die Programmparameter in der aktuellen Konfiguration geändert wurden (es wurden zum Beispiel neue Netzwerkfilter erstellt oder Einstellungen geändert), dann können diese Änderungen in einer beliebigen anderen bestehenden Konfiguration mit Ausnahme der Hauptkonfiguration gespeichert werden. Klicken Sie dazu mit der rechten Maustaste auf die benötigte Konfiguration und wählen im Kontextmenü den Befehl **Aktuelle Konfiguration speichern**. Klicken Sie im Fenster zur Bestätigung auf **Ja**.

In der aktuellen Konfiguration werden alle Änderungen automatisch gespeichert.

Wenn mehrere Konfigurationen im Programm definiert sind und in den Einstellungen das Kontrollkästchen **Konfigurationsfenster bei jedem Programmstart aufrufen** aktiviert ist, dann wird beim Start von ViPNet Monitor das Fenster zur Konfigurationsauswahl angezeigt.

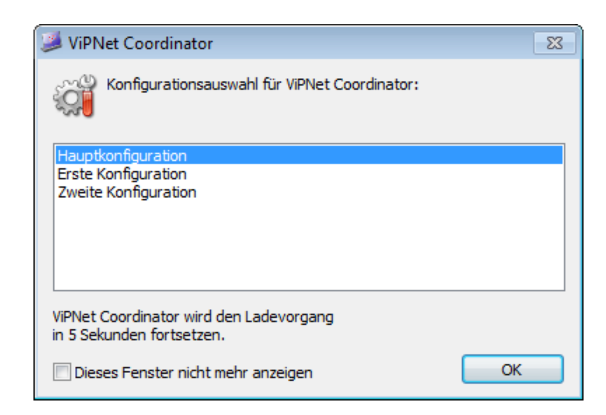


Abbildung 187. Konfigurationsauswahl beim Programmstart

Wenn Sie eine der Konfigurationen laden möchten, wählen Sie diese Konfiguration in der Liste aus und klicken Sie auf **OK**.

Wenn innerhalb 30 Sekunden, nachdem das Fenster auf dem Bildschirm angezeigt wurde, keine Konfiguration gewählt wird, setzt das Programm ViPNet Monitor die Arbeit mit der Einstellungen der Hauptkonfiguration fort.

Benutzerpasswort ändern

Es wird empfohlen, das Benutzerpasswort alle 3 Monate zu ändern. Im Allgemeinen wird die Häufigkeit des Passwortwechsels durch die Sicherheitsvorschriften des Unternehmens geregelt.

Im Programm ViPNet Client Monitor kann das Passwort über das Menü **Datei** > **Benutzerpasswort ändern** geändert werden. Bei Verwendung dieser Art des Passwortwechsels kann der Typ des Passworts nicht geändert werden. Außerdem kann das Benutzerpasswort des Programms ViPNet Client Monitor im Administratormodus geändert werden, wie weiter unten beschrieben.

Außerdem wird empfohlen, das Benutzerpasswort nach der primären Initialisierung bei der ersten Anmeldung im Programm ViPNet zu wechseln. Dies erhöht die Sicherheit des Passworts, da es dem Administrator nicht mehr bekannt sein wird.

Um das Benutzerpasswort zu ändern:

1 Wenn Sie das Programm ViPNet Client verwenden, dann wechseln Sie in den Administratormodus. Bei Verwendung des Programms ViPNet Coordinator ist die Anmeldung im Administratormodus nicht erforderlich.

2 Öffnen Sie im Fenster **Sicherheitseinstellungen** die Registerkarte **Passwort**.

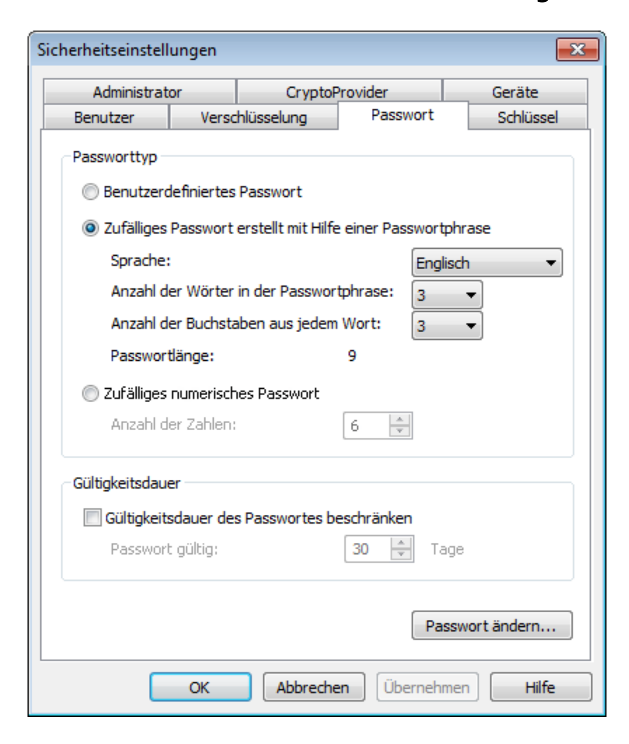


Abbildung 188. Aktuelles Benutzerpasswort ändern

3 Wählen Sie im Bereich **Passworttyp** den Typ aus, dem das neue Passwort entsprechen soll:

- **Benutzerdefiniertes Passwort** ist ein Passwort, das vom Benutzer definiert wird;
- **Zufälliges Passwort erstellt mit Hilfe einer Passwortphrase** ist ein Passwort, welches automatisch auf Basis einer Passwortphrase und nach vorgegebenen Parametern erstellt wird;

- **Zufälliges numerisches Passwort** ist ein Passwort, welches automatisch aus einer vorgegebenen Zahl von Ziffern erstellt wird.

4 Klicken Sie auf die Schaltfläche **Passwort ändern**. Führen Sie im eingeblendeten Fenster in Abhängigkeit vom gewählten Typ die Aktionen aus, die für den Passwortwechsel erforderlich sind.

5 Soll die Gültigkeitsdauer des neuen Passwortes begrenzt werden, aktivieren Sie das Kontrollkästchen **Gültigkeitsdauer des Passwortes beschränken** und geben gewünschte Anzahl von Tagen ein.

6 Klicken Sie auf **OK**.

Authentisierungsmodi

Im Programm ViPNet Monitor sind drei verschiedene Authentisierungsmodi vorgesehen: **Nur das Passwort**, **Passwort auf Authentisierungsgerät**, **PIN und Authentisierungsgerät**.



Achtung! Der Authentisierungsmodus **Passwort auf Authentisierungsgerät** entspricht nicht mehr den Sicherheitsanforderungen und wird ausschließlich aus Gründen der Kompatibilität mit früheren Versionen der ViPNet-Software unterstützt. Wenn also das Programm ViPNet Monitor auf die Version 4.x aktualisiert wurde und wenn dort der gegebene Authentisierungsmodus verwendet wird, dann empfehlen wir nachdrücklich, den Authentisierungsmodus auf **Nur das Passwort** oder **PIN und Authentisierungsgerät** zu ändern.

Standardmäßig ist der Modus **Nur das Passwort** eingestellt. Der Netzwerkknoten-Administrator kann in der Registerkarte **Schlüssel** im Fenster **Sicherheitseinstellungen** den Anmeldemodus ändern.

In einem der Modi **Passwort auf Authentisierungsgerät** oder **PIN und Authentisierungsgerät** erfolgt die Authentifizierung anhand eines externen Speichergeräts (s. Liste externer Datenträger auf S. 367). Um ein Gerät zur Authentifizierung verwenden zu können, soll darauf der notwendige Schlüssel gespeichert werden sowie auf dem Computer den entsprechenden Gerättreiber installiert werden.



Achtung! Wenn bei Verwendung des Authentisierungsmodus **Passwort auf Authentisierungsgerät** oder **PIN und Authentisierungsgerät** das externe Gerät vom Computer getrennt wird, dann wird automatisch der Computer gesperrt, der Traffic blockiert oder sowohl der Computer als auch der Traffic blockiert – in Abhängigkeit von den Einstellungen, die vom Administrator des Netzwerkknotens vorgenommen wurden. Zum Fortsetzen der Arbeit sollte das externe Gerät wieder an den Computer angeschlossen werden.

Führen Sie im Anmeldefenster von ViPNet Monitor die folgenden Schritte aus, um sich im Programm anzumelden:

1 Wählen Sie in Liste **Authentisierungsmodus** den Eintrag **Nur das Passwort** oder **PIN und Authentisierungsgerät**.

2 Wenn nötig, schließen Sie das externe Gerät an.

3 Wenn nötig, geben Sie Ihr Passwort im Feld **Passwort**.

4 Führen Sie folgende Aktionen durch, wenn Sie Authentisierungsgerät verwenden:

4.1 Wählen Sie in Liste **Authentisierungsgerät** das externe Gerät aus, auf dem sich Ihr privater Schlüssel oder das Zertifikat des privaten Signaturschlüssels befindet.

4.2 Wenn nötig, geben Sie eine PIN ein. Ob die Eingabe einer PIN erforderlich ist, hängt vom Typ des verwendeten externen Geräts ab. Damit die eingegebene PIN gemerkt wird und bei nachfolgenden Anmeldungen nicht mehr angegeben werden muss, aktivieren Sie das entsprechende Kontrollkästchen.

4.3 Wählen Sie in Gruppe **Authentifizierung mittels** eine der folgenden Optionen aus:

- **Zertifikat**: wenn Sie die Anmeldung mit Hilfe Ihres Zertifikats und des entsprechenden privaten Schlüssels durchführen möchten. Der private Schlüssel wird im Schlüsselcontainer auf dem verwendeten Gerät gespeichert. Wählen Sie in der Liste der auf dem Gerät gefundenen Zertifikate das benötigte Zertifikat aus.
- **Privater Schlüssel**: wenn Sie die Anmeldung mit Hilfe Ihres privaten Schlüssels durchführen möchten (der private Schlüssel ist Bestandteil der Benutzerschlüssel und wird auf dem verwendeten Gerät gespeichert).

5 Klicken Sie auf **OK**.

Benutzer–Authentisierungsmodus ändern

Der Authentisierungsmodus bestimmt, welche Daten ein Benutzer beim Login ins Programm ViPNet Monitor anzugeben hat. Um den Authentisierungsmodus zu ändern, gehen Sie wie folgt vor:

1 Melden Sie sich im Programm im Administratormodus an (s. Arbeiten mit Administratorrechten auf S. 338).

2 Klicken Sie auf die Schaltfläche **Ändern** in der Registerkarte **Schlüssel** im Fenster **Sicherheitseinstellungen**.

3 Wählen Sie einen der Modi im Fenster **Authentisierungsmodus** aus. Die Beschreibung möglicher Authentisierungsmodi sehen Sie im Abschnitt Authentisierungsmodi (auf S. 335).



Hinweis. Der Modus **Passwort auf Authentisierungsgerät** kann nicht ausgewählt werden, da er den aktuellen Sicherheitsanforderungen nicht mehr entspricht.

Falls die Authentifizierung mit Hilfe eines Zertifikats durchgeführt wird, schließen Sie dann das externe Gerät an und wählen anschließend das benötigte Zertifikat in der Liste der auf dem Gerät festgestellten Zertifikate aus.

Falls die Authentifizierung mit Hilfe eines privaten Schlüssels durchgeführt wird, schließen Sie dann das externe Gerät an, um den privaten Schlüssel des ViPNet Benutzers auf dem Gerät zu speichern. Beim Speichern des privaten Benutzerschlüssels (Schutzschlüssels (s. Schutzschlüssel auf S. 373)) auf einem externen Gerät sollte eine Besonderheit beachtet werden: wenn der Benutzer die Funktionen der Signatur und Verschlüsselung innerhalb von Anwendungen anderer Hersteller (zum Beispiel Microsoft Office) verwendet, dann wird es nachdrücklich empfohlen, den entsprechenden Schlüsselcontainer (auf S. 372) ebenfalls auf diesem Gerät zu speichern. Anderenfalls wird das Signieren und Verschlüsseln in Drittanwendungen nicht möglich sein, da es Probleme mit dem Zugang zum Schutzschlüssel geben wird. Der Schlüsselcontainer kann aus dem laufenden Ordner in einen anderen Ordner auf dem Laufwerk verschoben werden. In diesem Fall werden Sie jedoch jedes Mal beim Signieren und Verschlüsseln in einer Drittanwendung zur Passworteingabe aufgefordert.

4 Klicken Sie auf **OK**.

In der Registerkarte **Schlüssel** in der Gruppe **Authentifizierung** werden die Werte in den Feldern **Authentisierungsmodus** und **Authentisierungsgerät** entsprechend dem gewählten Modus geändert.

Arbeiten mit Administratorrechten

Ein Benutzer kann sich im Programm ViPNet Monitor im Administratormodus anmelden. Im diesem Modus sind folgende erweiterte Funktionen und Einstellungen verfügbar:

- Der Bereich **Administrator**, der in der Navigationsleiste des Programmfensters eingeblendet wird. In diesem Bereich können Sie erweiterte Einstellungen des ViPNet Netzwerkknotens vornehmen.
- Die Logdatei enthält Einträge über Ereignisse, die von einem Benutzer oder vom Administrator durchgeführt wurden.
- Möglichkeit zur Einsicht in die Logdatei der IP-Pakete eines bestimmten ViPNet Netzwerkknotens (s. Verwendung der Logdatei auf S. 324).
- Möglichkeit zur Anzeige und Änderung von Konfigurationen des Programms ViPNet Monitor (s. Steuerung von Programmkonfigurationen auf S. 331), die von allen Benutzern des Netzwerkknotens erstellt wurden.

Beim Arbeiten im Administratormodus werden alle Einschränkungen, die durch die aktuelle Berechtigungsstufe des Benutzers bedingt sind, wieder aufgehoben.

Wenn Sie sich im Programm im Administrator anmelden möchten:

1. Führen Sie einen der folgenden Schritte durch:
   - Wählen Sie im Programmfenster von ViPNet Monitor im Menü **ViPNet Client** oder **ViPNet Coordinator** den Eintrag **Als Administrator anmelden**.
   - Wählen Sie im Programmfenster von ViPNet Monitor im Menü **Service** den Eintrag **Sicherheitseinstellungen**.

     Öffnen Sie im Fenster **Sicherheitseinstellungen** die Registerkarte **Administrator** und klicken auf die Schaltfläche **Administratormodus-Login**.
2. Geben Sie das Administratorpasswort für den gegebenen ViPNet Netzwerkknoten im Fenster **Passwort** ein.

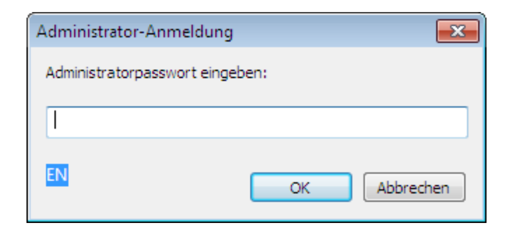


Abbildung 189. Passwort des Netzwerkknoten–Administrators eingeben

3. Klicken Sie auf die Schaltfläche **OK**.
4. Wenn das gegebene Passwort gültig ist, wird das Programm neu gestartet. Es stehen Ihnen nun zusätzliche Konfigurationsmöglichkeiten zur Verfügung.



Achtung! Das Passwort des Netzwerkknotenadministrators finden Sie im Programmfenster von ViPNet Network Manager im Bereich **Eigenes Netzwerk** auf der Registerkarte **Passwörter**.

Zusätzliche Sicherheitseinstellungen

Neben den erweiterten Einstellungen im Bereich **Administrator** sind im Administratormodus auch die folgenden Einstellungen in der Registerkarte **Administrator** im Fenster **Sicherheitseinstellungen** konfigurierbar:

- **Automatisch in ViPNet anmelden**: ermöglicht die Anmeldung im Programm ViPNet Monitor ohne vorhergehende Eingabe des ViPNet-Benutzerpassworts im Anmeldefenster des Programms. Wenn das Kontrollkästchen aktiviert ist, wird das Anmeldefenster beim Start des Programms auf dem aktuellen Netzwerkknoten nicht eingeblendet. Die Anmeldung in ViPNet Monitor erfolgt automatisch. Dies ist in den folgenden Fällen möglich:
  - bei Verwendung des Authentisierungsmodus **Nur das Passwort**: wenn das Passwort in der Registry gespeichert wird (d. h., das Kontrollkästchen **Passwort darf in der Registry gespeichert werden** ist aktiviert) und im Anmeldefenster des Programms das richtige Passwort angegeben und das Kontrollkästchen **Passwort speichern** aktiviert ist;
  - bei Verwendung des Authentisierungsmodus **Passwort auf Authentisierungsgerät** sowie **PIN und Authentisierungsgerät**: wenn das externe Gerät an den Computer angeschlossen ist und im Anmeldefenster des Programms die korrekte PIN angegeben und das Kontrollkästchen **PIN speichern** aktiviert ist.
- **Zertifikate aus dem Zertifikatsspeicher des Betriebssystems erlauben**: diese Einstellung ermöglicht neben der Verwendung der Zertifikate aus dem eigenen Zertifikatspeicher (Programmspeicher) auch die Verwendung der Zertifikate aus dem Zertifikatspeicher des Betriebsystems. Dies kann dann erforderlich sein, wenn in ViPNet Software der Cryptoprovider eines Drittherstellers (zum Beispiel CryptoPro) oder von externen Zertifizierungsstellen (außerhalb des ViPNet Netzwerks) herausgegebene Zertifikate verwendet werden sollen.
- **Nur eigenen Zertifikatlisten vertrauen**: wenn dieses Kontrollkästchen deaktiviert ist, wird die Suche nach dem Stammzertifikat bei der Zertifikatüberprüfung nicht nur im internen Zertifikatspeicher der ViPNet Software, sondern auch im Systemspeicher **Vertrauenswürdige Stammzertifizierungsstellen** und **Zwischenzertifizierungsstellen** durchgeführt.
- **Ignorieren, wenn die Zertifikatsperrlisten nicht vorhanden sind**: dieses Kontrollkästchen sollte dann aktiviert werden, wenn im System Zertifikate verwendet werden, die von einer externen Zertifizierungsstelle veröffentlicht wurden, da Informationen über Zertifikatsperrlisten in solchen Zertifikaten fehlen können.

Einsicht in der Logdatei

Einschränkung der Verwendungsmöglichkeiten des Programms ViPNet Monitor

- Änderung der Netzwerkfilter.
- An- und Abmeldung eines Benutzers.
- Anmeldung im Administratormodus.
- Konfigurationsänderung.
- Andere Ereignisse.

Diese Informationen ermöglichen es dem Administrator, die Einhaltung der Sicherheit zu kontrollieren.

Um die Ereignis-Logdatei einzusehen:

1. Melden Sie sich im Programm im Administratormodus an (s. Arbeiten mit Administratorrechten auf S. 338).
2. Wählen Sie den Bereich **Administrator** in der Navigationsleiste des Programmfensters ViPNet Monitor aus.
3. Klicken Sie im Bereich **Administrator** auf die Schaltfläche **Logdatei**.

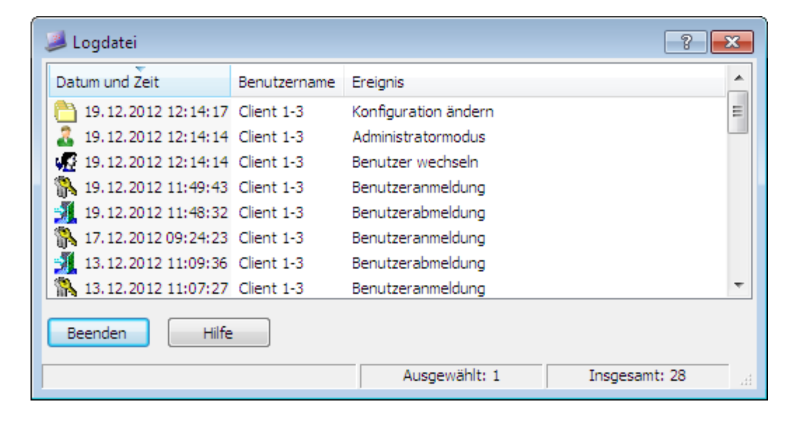


Abbildung 190. Einsicht in der Logdatei

4. Zur Ansicht der Logdatei im HTML- oder XLS-Format klicken Sie im Fenster Logdatei auf eine beliebige Zeile mit der rechten Maustaste und wählen im geöffneten Kontextmenü die Option **In HTML-Format anzeigen** oder **In Excel-Format anzeigen** (vorausgesetzt das Programm Microsoft Excel ist auf dem Computer installiert) aus.



Versionsgeschichte von ViPNet VPN

In dieser Anwendung werden die wichtigsten Änderungen in den vorherigen Versionen von ViPNet Network Manager beschrieben.

Version 4.2.2

In diesem Abschnitt wird eine kurze Übersicht der Änderungen und neuen Möglichkeiten der Version 4.2.2 geboten.

- **Unterstützung weiterer Modifikationen von ViPNet Coordinator HW/VA**

  Nun können Sie in Ihrem Netzwerk die Appliances ViPNet Coordinator HW100 und HW100 Advanced (s. Modifikationen von ViPNet Coordinator HW auf S. 34) sowie virtuelle Komponenten ViPNet Coordinator VA100, VA1000, VA2000 (s. Modifikationen von ViPNet Coordinator VA auf S. 34) einsetzen, sofern Sie eine passende Lizenz dafür besitzen.

  Alle Modifikationen von ViPNet Coordinator HW und ViPNet Coordinator VA übernehmen die gleichen Aufgaben im Netzwerk. Die grundliegenden Unterschiede zwischen den vorhandenen Modifikationen sind durch die Begrenzungen der Leistungsfähigkeit der Coordinatoren und der Anzahl der unterstützten Netzwerkadapter bedingt.

- **Unterstützung der ViPNet Failover Technologie**

  Bei der Verwendung von Coordinator VA100, VA1000 oder VA2000 steht Ihnen nun die ViPNet Failover Funktion zur Verfügung, die Sie bei Bedarf aktivieren können. Die ViPNet Failover Technologie ermöglicht es Ihnen, einen fehlertoleranten Cluster aus zwei ViPNet Coordinator VA Komponenten aufzubauen.

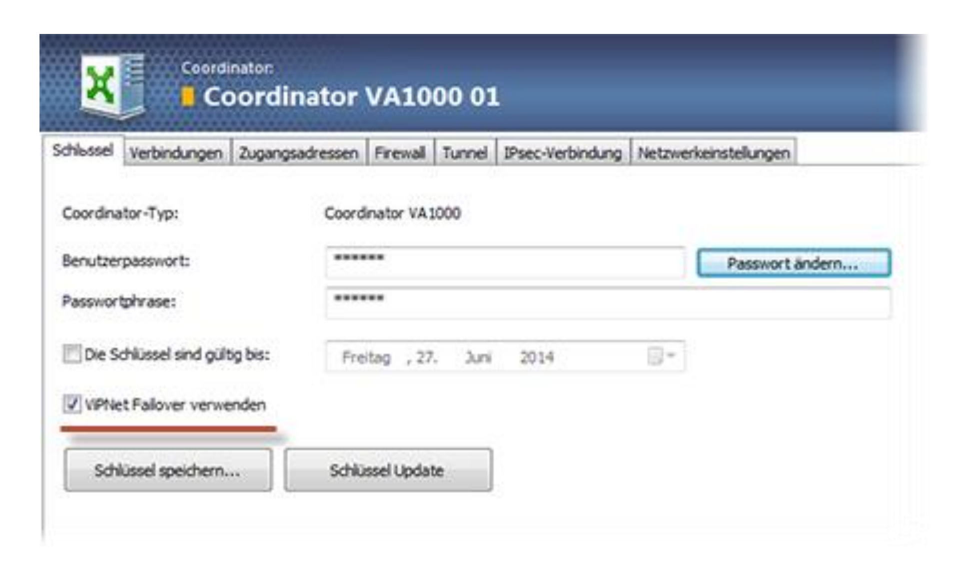


Abbildung 191. ViPNet Failover Funktion aktivieren

- **Konfiguration der Liste der verwalteten Knoten für das ViPNet Policy Manager**

  Erlauben Sie die Nutzung der Software ViPNet Policy Manager auf dem Client, ist es erforderlich, die Liste der Netzwerkknoten anzugeben, deren Sicherheitslinien Sie mit Hilfe des ViPNet Policy Managers verwalten können.

- **Anzeige und Wechsel des Netzwerkknotenadministrator-Passworts**

  In den vorhergehenden Versionen des Programms ViPNet Network Manager wurde das Passwort des Netzwerkknotenadministrators (s. Netzwerkknotenadministrator-Passwort auf S. 371) ausschließlich in der Datei `ViPNet_a.txt` gespeichert, die gleichzeitig mit den Netzwerkknotenschlüsseln automatisch erstellt wurde und nicht geändert werden konnte. In Version 4.2.2 besteht die Möglichkeit, das Passwort im Programm ViPNet Network Manager anzuzeigen und zu ändern (s. Wechsel des Internetzwerk-Masterschlüssels auf S. 179). Die Datei `ViPNet_a.txt` wird nicht mehr angelegt.

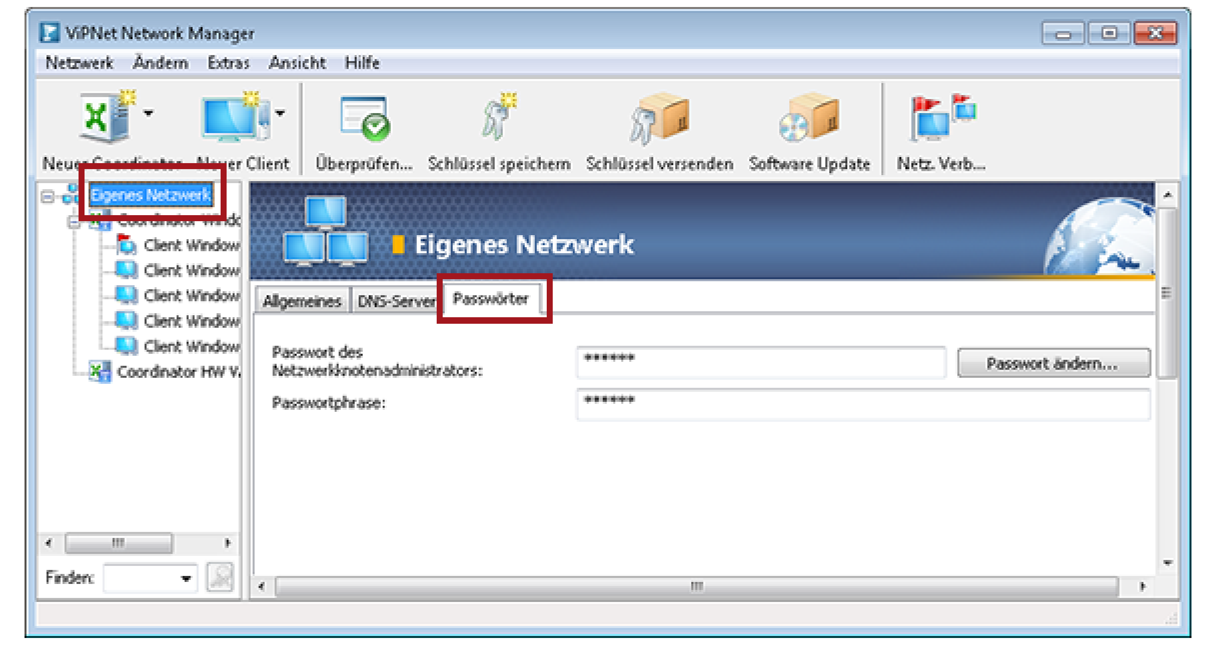


Abbildung 192. Wechsel des Netzwerkknotenadministrator-Passworts

- **Wechsel des Internetzwerk-Masterschlüssels**

  Damit die Sicherheit der Partnernetzwerk-Kommunikation erhöht wird, gibt es nun die Möglichkeit der Änderung des Internetzwerk-Masterschlüssels, der für abgesicherte Partnernetzwerk-Verbindungen verwendet wird.

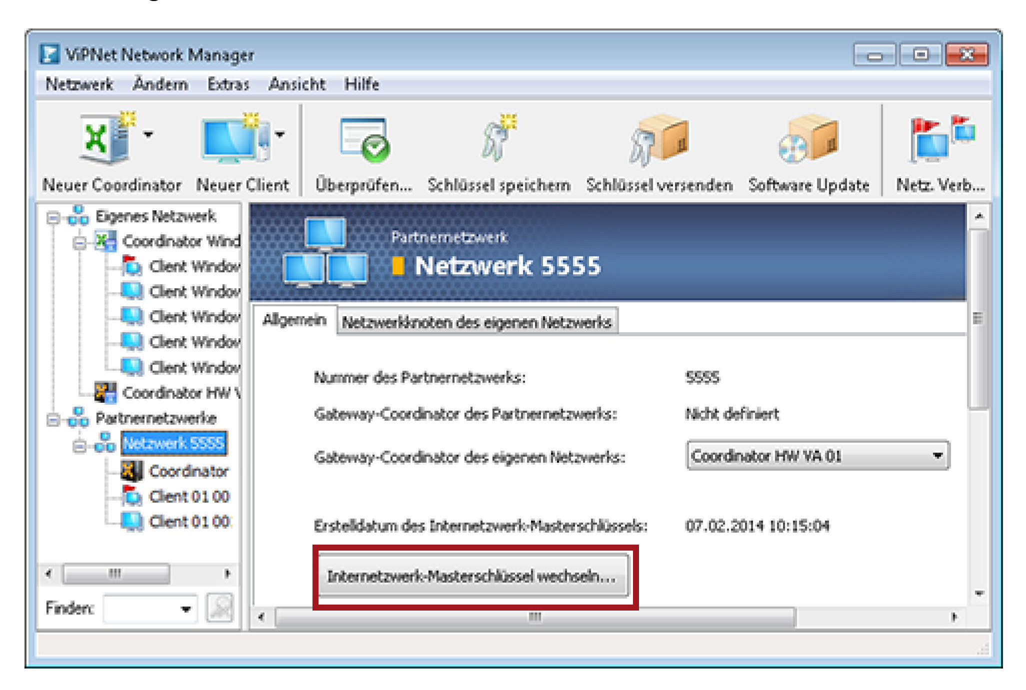


Abbildung 193. Wechsel des Internetzwerk-Masterschlüssels

Version 4.2

In diesem Abschnitt wird eine kurze Übersicht der Änderungen und neuen Möglichkeiten der Version 4.2 geboten.

- **Änderung des Namens der Softwarelösung ViPNet OFFICE**

  Der Name des Softwarepakets ViPNet OFFICE wurde auf ViPNet VPN geändert. Zusätzlich wurden die folgenden Anwendungen umbenannt:

  - das Programm ViPNet Manager wurde in ViPNet Network Manager umbenannt;
  - Die Software ViPNet Security Gateway wurde folgendermaßen umbenannt:
    - die für die Installation auf den Computer bestimmte Version trägt den Namen ViPNet Coordinator HW;
    - die für die Bereitstellung in einer virtuellen Umgebung bestimmte Version trägt den Namen ViPNet Coordinator VA.

- **Gesonderte Berücksichtigung von Lizenzen für unterschiedliche Arten von Clients und Coordinatoren**

  Beim Hinzufügen von Clients und Coordinatoren zum Netzwerk wurde bisher sowohl die Gesamtanzahl an verfügbaren Lizenzen für Clients und Coordinatoren als auch die Anzahl an freien

Lizenzen für bestimmte Typen von Clients und Coordinatoren verringert. Beispiel: beim Erstellen des Coordinators ViPNet Coordinator HW/VA wurde sowohl die Anzahl an freien Lizenzen für alle Coordinatoren (Gesamtanzahl) als auch die Anzahl der Lizenzen für Coordinatoren vom Typ ViPNet Coordinator HW/VA herabgesetzt. Nun wird die Berechnung der Anzahl an freien Lizenzen für Clients und Coordinatoren für jeden Typ getrennt durchgeführt.

- **Änderung der Lizenzeinschränkungen für die Testversion von ViPNet VPN**

  Die Lizenzeinschränkungen für die Testversion von ViPNet VPN wurden gelockert. Nun können mit Hilfe einer nicht registrierten Version von ViPNet Network Manager alle Typen von Coordinatoren und Clients erstellt werden. Ebenso ist der Einsatz der Programme ViPNet Policy Manager, ViPNet Business Mail und ViPNet SafeDisk-V möglich. Mit Hilfe der Softwarelösung ViPNet StateWatcher (auf S. 38) können außerdem bis zu zehn Knoten überwacht werden.

- **Vereinfachung der Netzwerkknoten-Einstellungen**

  Früher war für die Konfiguration der Netzwerkknoten im Programm ViPNet Network Manager die Ausführung zahlreicher Schritte notwendig, was für den Netzwerkadministrator einige Schwierigkeiten verursachen konnte. Nun wurde die Vorgehensweise bei der Konfiguration der Netzwerkknoten überarbeitet und wesentlich vereinfacht:

  - Die Konfiguration der IP-Adressen und DNS-Namen der Coordinatoren sowie die Konfiguration der IP-Adressen und DNS-Namen der Coordinator-Firewall wird nun auf einer Registerkarte **Zugangsadressen** durchgeführt.
  - Eine zentralisierte Konfiguration der Firewall der Clients wird nicht mehr durchgeführt.
  - Die Auswahl des Client- oder Coordinatortyps wird nun unmittelbar beim Erstellen des Netzwerkknotens durchgeführt. Nach dem Erstellen des Knotens kann sein Typ nicht mehr geändert werden.



Abbildung 194. Erstellen des neuen Netzwerkknotens

  - Die Konfiguration der IP-Adressen und DNS-Namen der Clients sowie die Konfiguration der externen IP-Adressen der Client-Firewalls ist nicht mehr erforderlich.
  - Als IP-Adressenserver für die Clients werden standardmäßig ihre Coordinatoren verwendet. Es ist nicht mehr nötig, den IP-Adressenserver in der Registerkarte **IP-Adressen** anzugeben.
  - Die Konfiguration der Speicherung des Passworts auf den Knoten wurde vereinfacht und wird nun auf der Registerkarte **Schlüssel** durchgeführt.

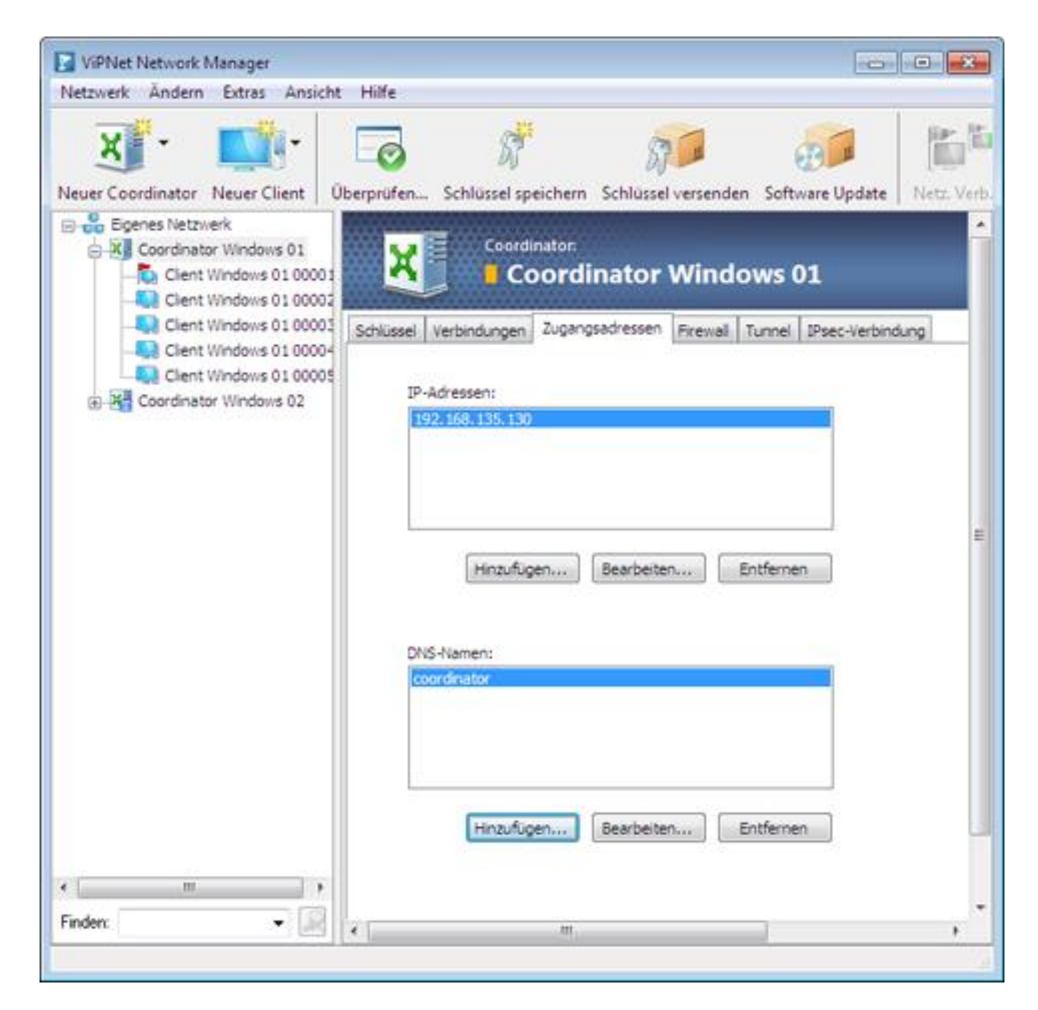


Abbildung 195. Zugangsadressen des Coordinators

- **Keine Funktion zur Verwaltung der Berechtigungen**

  Früher wurden im Programm ViPNet Network Manager die Berechtigungen der ViPNet Netzwerkbenutzer konfiguriert. Nun wird diese Funktionalität nicht mehr verwendet. Standardmäßig wird den Coordinatoren des Netzwerks die Berechtigungsstufe „Standardmodus", den Clients die Berechtigungsstufe „Eingeschränkter Modus" zugewiesen. Auf den Coordinatoren kann die Berechtigungsstufe vom Netzwerkknotenadministrator geändert werden. Beim Update von ViPNet VPN auf die Version 4.2 wird allen Clients die Berechtigungsstufe „Eingeschränkter Modus" zugewiesen. Auf den Coordinatoren wird die zuvor eingestellte Berechtigungsstufe beibehalten.

- **Unterstützung der Software ViPNet Client und ViPNet Coordinator der Version 4.2**

  Zuvor wurde vom Programm ViPNet Network Manager die Software ViPNet Client und ViPNet Coordinator der Version 4.1 unterstützt. Nun besteht die Möglichkeit, diese Software in der Version 4.2 auf die Knoten zu installieren.

  Weitere Informationen zu den neuen Möglichkeiten der Software ViPNet Client und ViPNet Coordinator finden Sie im Dokument „Neue Möglichkeiten von ViPNet Client und ViPNet Coordinator Version 4.x. Anhang zur ViPNet Dokumentation".

- **Verwendung des Programms ViPNet Client mit vereinfachter Oberfläche**

  Früher wurde das Programm ViPNet Client mit seiner vollständigen Benutzeroberfläche auf den Netzwerkclients verwendet. Eine hohe Anzahl an Funktionen und Einstellungen des Programms

konnte zu Schwierigkeiten auf Seiten der Benutzer führen. Nun wird auf den Clients das Programm ViPNet Client mit einer reduzierten Oberfläche verwendet. Mit Hilfe dieser Oberfläche kann der Benutzer mit der Liste der geschützten Knoten arbeiten, Nachrichten und Dateien mit anderen Benutzern austauschen und Updates der Adresslisten und Schlüssel annehmen. Alle Funktionen zur Konfiguration des Programms werden dabei vom Netzwerkknotenadministrator ausgeführt.

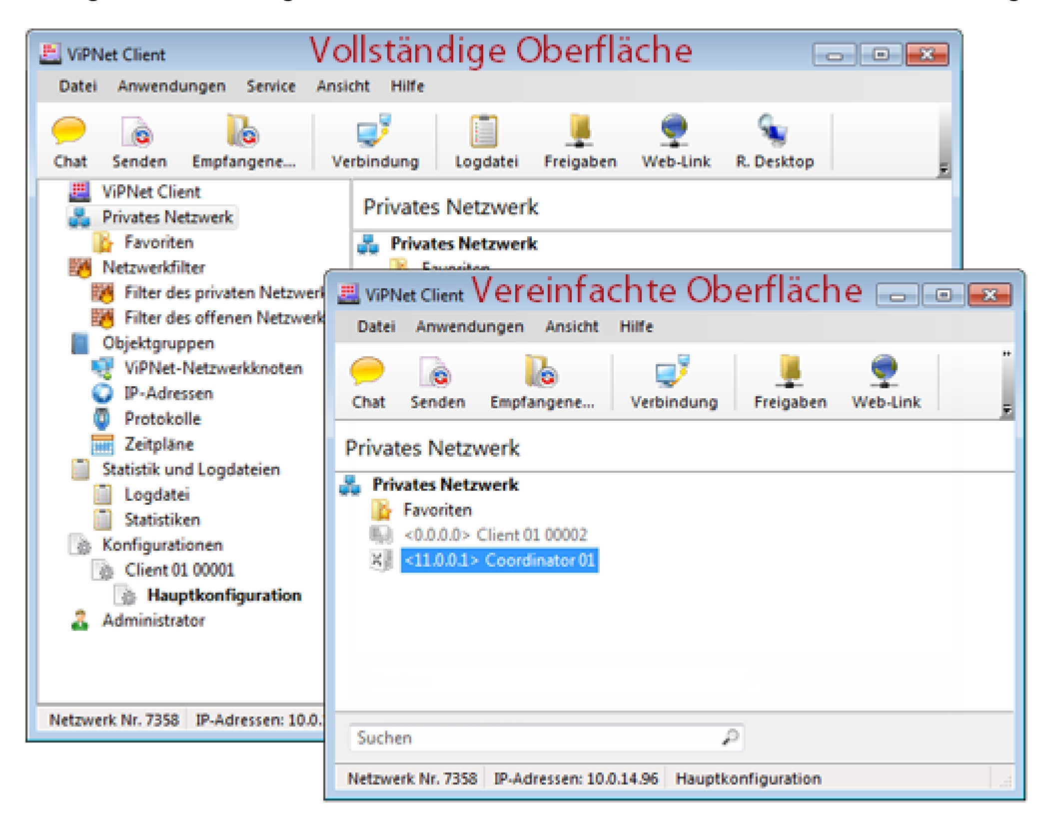


Abbildung 196. Benutzeroberfläche des Programms ViPNet Client Monitor

- **Definition der Netzwerkeinstellungen von ViPNet Coordinator HW/VA**

  Es besteht nun die Möglichkeit, die Netzwerkeinstellungen für den Coordinator ViPNet Coordinator HW/VA im Programm ViPNet Network Manager zu konfigurieren. Sie können dort die Parameter der Netzwerkadapter von ViPNet Coordinator HW/VA angeben und die Routen für die Weiterleitung des Traffics über diesen Coordinator definieren. Die aktualisierten Einstellungsdaten von ViPNet Coordinator HW/VA werden als Bestandteil von Adresslisten weitergeleitet.

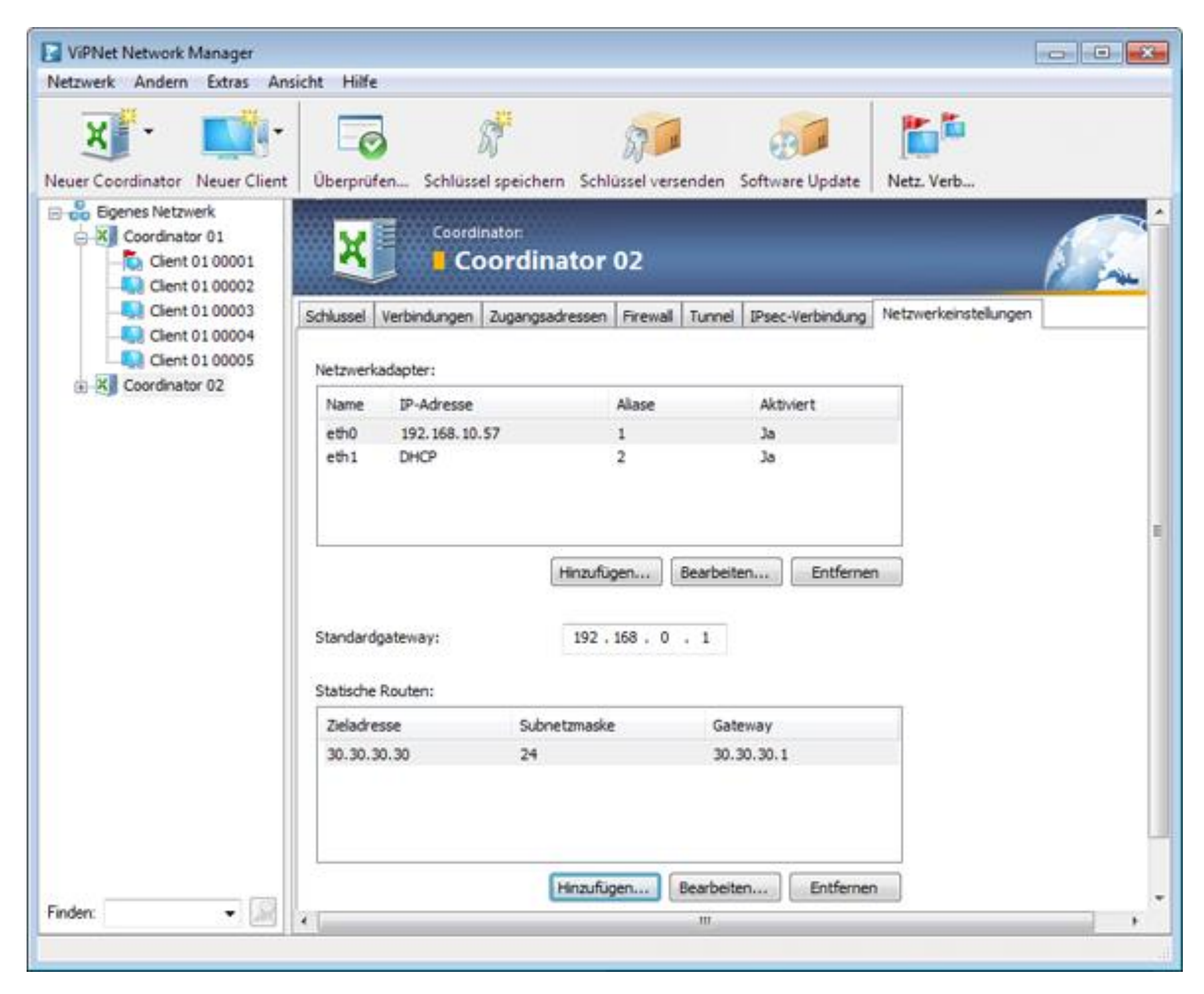


Abbildung 197. Konfiguration von ViPNet Coordinator HW/VA

- **Geänderte Oberfläche des Programms ViPNet Network Manager**

  Wegen der Vereinfachung der Vorgehensweise beim Konfigurieren der Netzwerkknoten und einigen Änderungen in anderen Funktionen wurde die Oberfläche des Programms ViPNet Network Manager überarbeitet.

Tabelle 16. Grundlegende Änderungen in der Benutzeroberfläche

Was wurde geändert	Version 4.0	Version 4.2
Registerkarten **Firewall des Clients**, **Benutzerrechte** sowie **IP-Adressen** und **DNS-Namen** der Clients	Vorhanden	Fehlt
Registerkarten **IP-Adressen** und **DNS-Namen** der Coordinatoren	Zwei separate Registerkarten	Zu einer Registerkarte **Zugangsadressen** zusammengeführt
Registerkarte **Netzwerkeinstellungen** für ViPNet Coordinator HW/VA	Fehlt	Vorhanden

Was wurde geändert	Version 4.0	Version 4.2
Konfiguration der Speicherung des Passworts auf den Knoten	Registerkarte **Benutzerrechte**	Registerkarte **Schlüssel**
Konfiguration der externen Adressen der Firewalls	Registerkarte **Firewall**	Für Coordinatoren auf der Registerkarte **Zugangsadressen**, für Clients wird diese Funktion nicht durchgeführt
Auswahl des VPN-Servers für die Clients	Registerkarte IP-Adressen	Wird nicht durchgeführt
Konfiguration der Verwendung von ViPNet Business Mail	Fehlt	Registerkarte **Schlüssel**
Konfiguration der maximalen Anzahl an getunnelten Verbindungen	Registerkarte **Tunnel**	Wird nicht durchgeführt
Netzwerkaufbau-Assistent		Seiten mit den Verbindungseinstellungen von Coordinatoren wurden geändert

- **Möglichkeit der Verwendung der Software ViPNet StateWatcher und ViPNet Policy Manager an Clients mit dem Typ ViPNet Client Windows**

  Früher konnten die Programme ViPNet StateWatcher und ViPNet Policy Manager automatisch auf dem Client verwendet werden, der als Manager-Arbeitsplatz festgelegt war. Nun besteht die Möglichkeit, diese Rollen anderen Clients des ViPNet Netzwerks zuzuweisen (mit Ausnahme der Knoten ViPNet Client for Mac OS X, ViPNet ThinClient und mobiler Clients (s. Verwendung der Software ViPNet StateWatcher auf S. 120)).

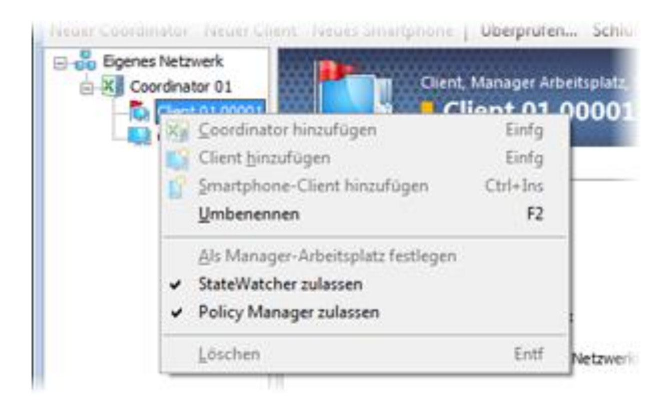


Abbildung 198. Verwendung der Software ViPNet StateWatcher und ViPNet Policy Manager aktivieren

- **Unterstützung von ViPNet ThinClient**

Es kann nun die integrierte Hard- und Softwarelösung ViPNet ThinClient als Netzwerkclient eingesetzt werden. ViPNet ThinClient wird zum Bereitstellen geschützter Benutzer-Arbeitsstationen verwendet und erfüllt die Funktionen eines Terminalclients. Dabei wird die Verschlüsselung und die Filterung des IP-Traffics sichergestellt (s. ViPNet ThinClient auf S. 36).

- **Unterstützung von ViPNet Client Android**

  Es besteht nun die Möglichkeit, die Software ViPNet Client Android (s. ViPNet Client for Android auf S. 35) auf den Clients im ViPNet Netzwerk zu verwenden. Mit Hilfe der Software ViPNet Client Android können Clients zum ViPNet Netzwerk hinzugefügt werden, die unter der Steuerung des Betriebssystems Android arbeiten. Ein Client dieses Typs kann nicht als Manager-Arbeitsplatz festgelegt werden.

- **Aufhebung der Lizenzeinschränkung für die Anzahl der getunnelten Verbindungen**

  Früher konnte im Programm ViPNet Network Manager nur eine bestimmte Anzahl der Tunnel definiert werden, die von der Lizenz für ViPNet VPN begrenzt war. Nun wurde die Lizenzeinschränkung für die Anzahl der Tunnel aufgehoben. Beim Update von ViPNet VPN einer früheren Version wird die vorhandene Begrenzung für die Anzahl an gleichzeitig getunnelten Knoten für alle Coordinatoren gelöscht.

- **Lizenzierung der Verwendung des Programms ViPNet Business Mail**

  Im Programm ViPNet Network Manager wurde eine Lizenzeinschränkung für die Verwendung des Programms ViPNet Business Mail eingeführt. Bei der Installation der Software ViPNet Client wird das Programm ViPNet Business Mail nun nicht mehr standardmäßig auf den Client installiert. Für die Installation und Verwendung dieses Programms auf den Netzwerkclients sollte im Programm ViPNet Network Manager für alle betroffenen Clients auf der Registerkarte **Schlüssel** das Kontrollkästchen **Business Mail verwenden** aktiviert werden. Dann sollten Schlüsselupdates an die Knoten versendet werden. Anschließend kann das Programm ViPNet Business Mail auf die benötigten Clients installiert werden.

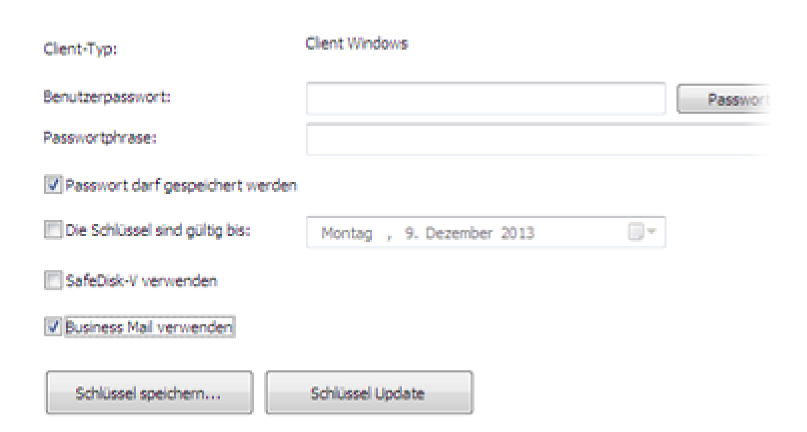


Abbildung 199. Verwendung der Software ViPNet Business Mail erlauben

- **Keine Funktion zum Erstellen des Stammzertifikats**

  Da die Public-Key-Infrastruktur (PKI) nicht in ViPNet VPN-Netzwerken verwendet wird, besteht auch keine Notwendigkeit, Stammzertifikate für den Administrator des Netzwerks zu erstellen. Beim Aufbau des Netzwerks und der Knotenschlüssel im Programm ViPNet Network Manager wird nun kein Stammzertifikat mehr angelegt.

- **Möglichkeit zur Änderung des Benutzerpassworts während beliebiger Sitzung im Programm ViPNet Network Manager**

  Im Programm ViPNet Network Manager konnten die Benutzerpasswörter zuvor ausschließlich in der Programmsitzung geändert werden, in welcher die Netzwerkknoten erstellt wurden. Nun wurde diese Einschränkung aufgehoben. Wenn eine Schlüsseldistribution auf dem Knoten bereits installiert ist, dann wird nach dem Passwortwechsel zusammen mit dem Schlüsselupdate eine Benachrichtigung an den Client gesendet, dass der Benutzer sein Passwort selbständig ändern sollte. Das Passwort, das vom Administrator im Programm ViPNet Network Manager definiert wurde, wird nicht an den Knoten weitergeleitet.

Version 4.0.1

In diesem Abschnitt wird eine kurze Übersicht der Änderungen und neuen Möglichkeiten der Version 4.0.1 geboten.

- **Unterstützung der Software ViPNet Client und ViPNet Coordinator Version 4.1**

  Früher wurde vom Programm ViPNet Network Manager die Software ViPNet Client und ViPNet Coordinator der Version 4.0 unterstützt. Nun kann die gegebene Software in der Version 4.1 auf die Knoten installiert werden.

  Informationen zu den neuen Möglichkeiten der Software ViPNet Client und ViPNet Coordinator finden Sie im Dokument „Neue Möglichkeiten von ViPNet Client und ViPNet Coordinator Version 4.x. Anhang zur ViPNet Dokumentation“.

- **Korrektur der Fehler**

  Es wurden Fehler behoben, die beim Einsatz vorhergehender Programmversionen von ViPNet Network Manager festgestellt wurden.

Version 4.0

In diesem Abschnitt wird eine kurze Übersicht der Änderungen und neuen Möglichkeiten der Version 4.0 geboten.

- **Unterstützung der Software ViPNet Client und ViPNet Coordinator der Version 4.0**

  Vom Programm ViPNet Network Manager wurde zuvor die Software ViPNet Client und ViPNet Coordinator der Version 3.2.x unterstützt. Nun besteht die Möglichkeit, diese Software in der Version 4.0 auf die Netzwerkknoten zu installieren. Weitere Informationen zu den neuen Möglichkeiten der Software ViPNet Client und ViPNet Coordinator finden Sie im Dokument „Neue Möglichkeiten von ViPNet Client und ViPNet Coordinator Version 4.0. Anhang zur ViPNet Dokumentation“.

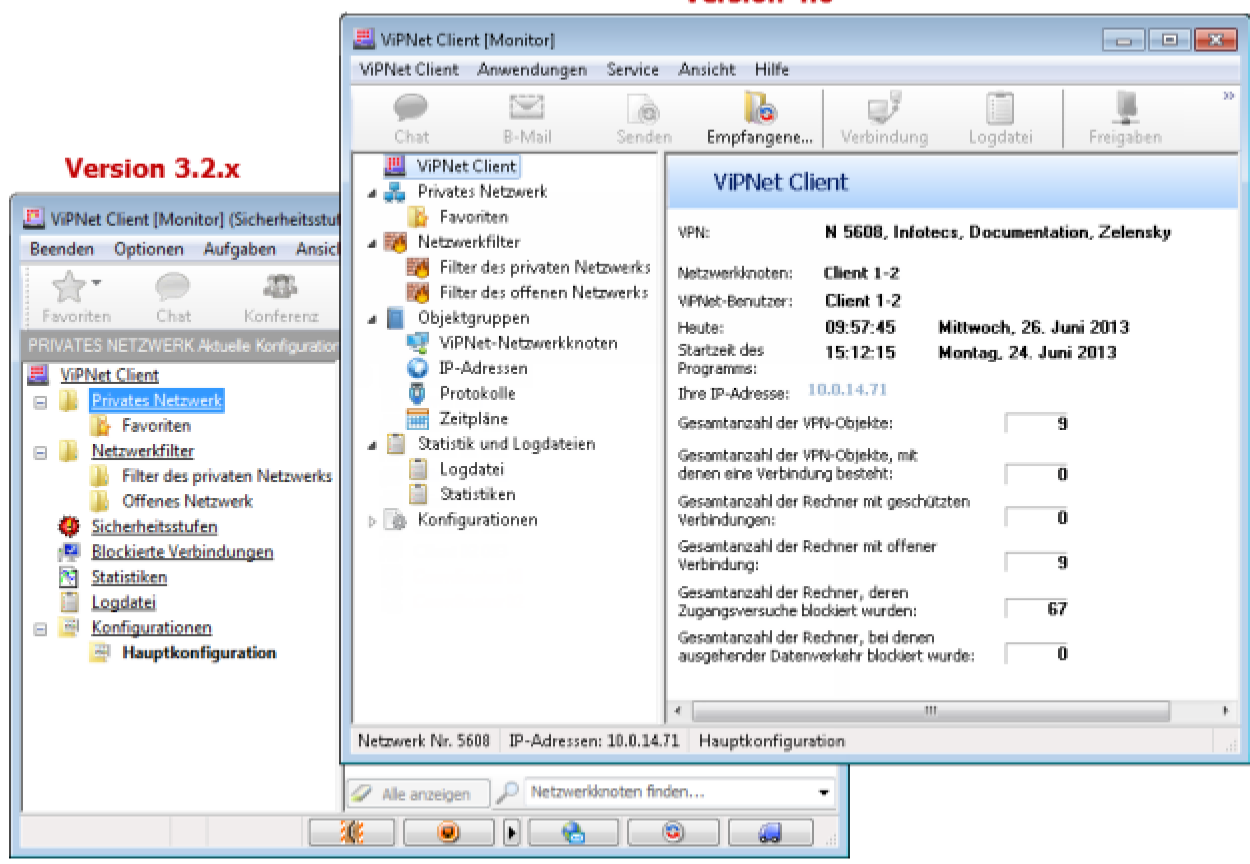


Abbildung 200. Änderungen in der Oberfläche von ViPNet Monitor

- **Unterstützung der Software ViPNet Client for Mac OS X**

  Vom Programm ViPNet Network Manager wurde zuvor die Software ViPNet Client für Windows unterstützt. Nun besteht die Möglichkeit, die Software ViPNet Client for Mac OS X auf den Netzwerkknoten zu verwenden. Für die Clients dieses Typs werden die Software- und Schlüsselupdates nicht gemeinsam mit den Updates anderer Knoten versendet, sondern vom Netzwerkadministrator separat weitergeleitet. Außerdem können Clients dieses Typs nicht als Manager-Arbeitsplatz eingerichtet werden.

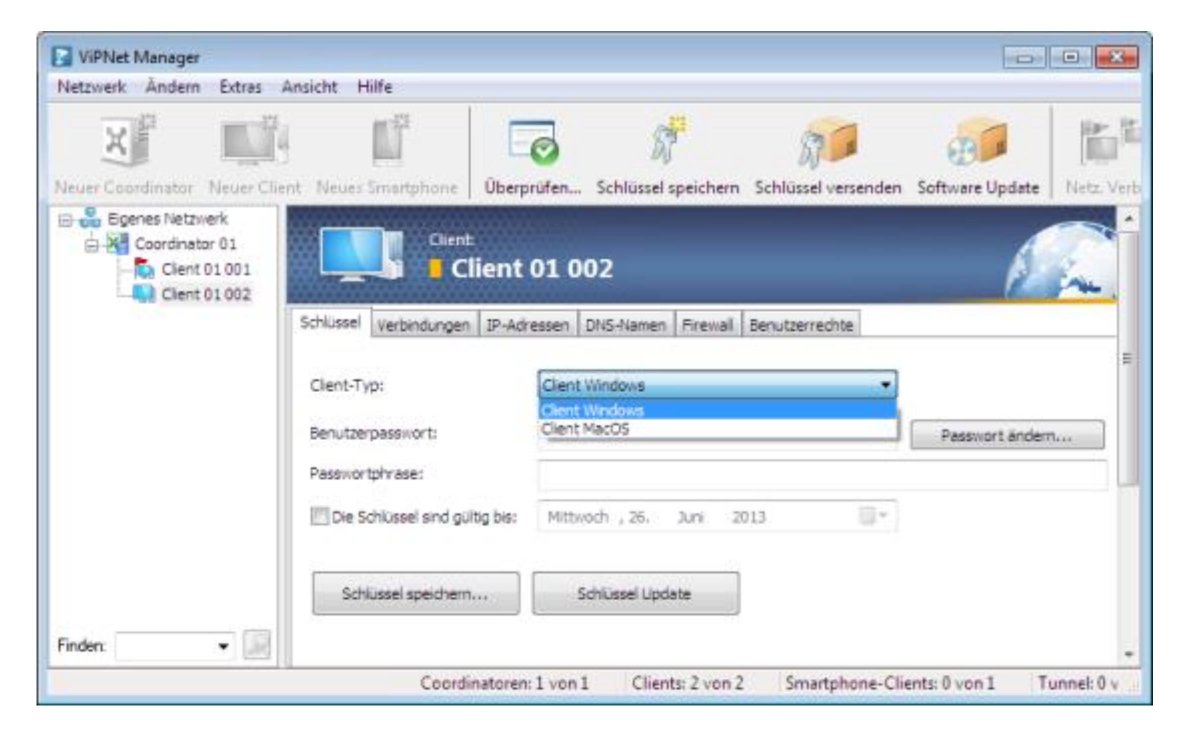


Abbildung 201. Auswahl des Clienttyps

- **Verwendung des Softwaresystems ViPNet StateWatcher**

  Im ViPNet VPN-Netzwerk kann nun das Softwaresystem ViPNet StateWatcher verwendet werden (s. ViPNet StateWatcher auf S. 38). Dieses Softwaresystem dient der Überwachung der Netzwerkknoten mit dem Ziel, Daten über den Status der Knoten zu ermitteln und mögliche Fehler im Betrieb der Knoten aufzudecken.

  Die Software Monitoring Server wird als Basiskomponente des Softwaresystems ViPNet StateWatcher auf die Arbeitsstation des ViPNet Netzwerkadministrators installiert. Diese Software kann über die Web-Schnittstelle Monitoring-Arbeitsplatz von jedem beliebigen geschützten Netzwerkknoten gesteuert werden.

- **Verwendung des Programms ViPNet Policy Manager**

  Es besteht nun die Möglichkeit, die Sicherheitsrichtlinien der Netzwerkknoten, auf denen die Software ViPNet Client und ViPNet Coordinator installiert ist, mit Hilfe des Programms ViPNet Policy Manager (auf S. 37) zentralisiert zu verwalten. Dieses Programm wird auf dem Manager-Arbeitsplatz installiert.

- **Definition der DNS-Serverliste**

  Es kann nun eine Liste von DNS-Servern festgelegt werden, die auf den Knoten des lokalen ViPNet Netzwerks installiert sind. Als DNS-Server können folgende Knotentypen auftreten:

  - ViPNet Coordinator (Windows).
  - ViPNet Coordinator HW/VA.
  - ViPNet Client (Windows) einschließlich des Knotens, auf dem der Manager-Arbeitsplatz eingerichtet ist.

  Knoten, die von Coordinatoren getunnelt werden, können ebenfalls als DNS-Server auftreten.

- **Import der Lizenzdatei**

Zur Aktualisierung der Netzwerklizenz musste bis jetzt die Datei `infotecs.reg` in den Installationsordner von ViPNet Network Manager kopiert und das Programm neu gestartet werden. Nun kann die Lizenzdatei unmittelbar im Programmfenster von ViPNet Network Manager importiert werden. Wählen Sie im Menü **Hilfe** den Befehl **Lizenzdatei laden** (s. Import der neuen Lizenz auf S. 49), um die Lizenzdatei zu importieren.

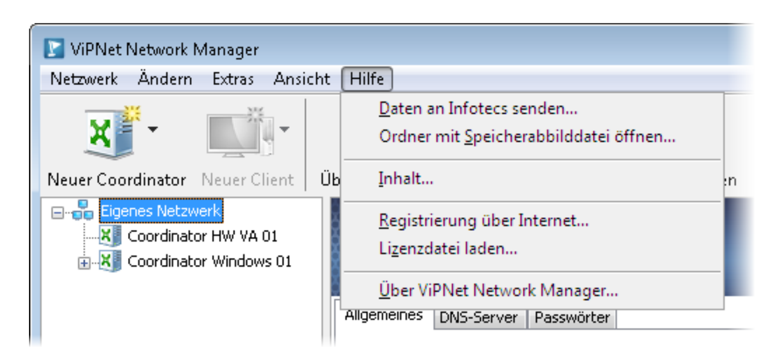


Abbildung 202. Import der Lizenzdatei

- **Möglichkeit zum Deaktivieren der Überprüfung der Datenvollständigkeit**

  Während der Konfiguration und Bearbeitung der Netzwerkstruktur deckt das Programm ViPNet Network Manager mögliche Konflikte auf und weist auf fehlende Daten hin. Nun besteht die Möglichkeit, diese Prüfung auf unvollständige Daten zu deaktivieren (s. Erkennen von unvollständigen Daten deaktivieren auf S. 130), damit erfahrene ViPNet Netzwerkadministratoren von den eingeblendeten Hinweisen nicht abgelenkt werden. Die Prüfung der Datenvollständigkeit kann im Fenster **Einstellungen** oder im Fenster **Überprüfung der ViPNet Netzwerkkonfiguration** deaktiviert werden.



Abbildung 203. Deaktivieren der Überprüfung der Datenvollständigkeit

- **Erstmaliger Start des Programms ViPNet Network Manager ohne Netzwerk-Erstellung**

Beim erstmaligen Starten des Programms ViPNet Network Manager musste zuvor sofort die Netzwerkstruktur mit Hilfe des ViPNet Netzwerkaufbauassistenten erstellt werden. Nun können Sie diesen Schritt überspringen und sofort zum Hauptfenster des Programms wechseln. Klicken Sie dazu im Assistentenfenster auf die Schaltfläche **Schließen**. Dabei wird eine Mindeststruktur des Netzwerks angelegt (ein Coordinator und ein Client, der als Manager-Arbeitsplatz festgelegt wird) und das Hauptfenster von ViPNet Network Manager geöffnet.

Version 3.0.6

In diesem Abschnitt wird eine kurze Übersicht der Änderungen und neuen Möglichkeiten der Version 3.0.6 geboten.

- **Korrektur der Fehler**

  Fehler, die bei Verwendung vorheriger Programmversionen festgestellt wurden, wurden behoben

- **Aktualisierung der Dokumentation und Hilfe**

  Dokumentation und Hilfe von ViPNet VPN wurden ergänzt.

Version 3.0.5

In diesem Abschnitt wird eine kurze Übersicht der Änderungen und neuen Möglichkeiten der Version 3.0.5 geboten.

- **Installation von ViPNet Network Manager auf dem Coordinator**

  Das Programm ViPNet Network Manager kann nun sowohl auf einem Client als auch auf dem Coordinator installiert werden (zum Beispiel wenn in einem kleinen ViPNet Netzwerk das Reservieren eines eigenen Clients für die Arbeitsstation des Administrators nicht zweckmäßig erscheint).

- **Übertragung der Arbeitsstation des ViPNet Administrators auf einen anderen Knoten**

  Der Manager-Arbeitsplatz (Arbeitsstation des Administrators) kann nun zusammen mit allen erforderlichen Daten über das installierte ViPNet Netzwerk und den Programmeinstellungen von ViPNet Network Manager von einem Netzwerkknoten auf einen anderen verlegt werden.

- **Änderung der Benutzeroberfläche des Installationsprogramms von ViPNet VPN und des ViPNet Netzwerkaufbau-Assistenten**

  Da nun die Möglichkeit besteht, ViPNet Network Manager auf dem Coordinator zu installieren, wurde auf der Benutzeroberfläche des Installationsprogramms von ViPNet VPN die Funktion zur Installation der Software ViPNet Coordinator auf der Arbeitsstation des Administrators hinzugefügt.



Abbildung 204. Erstellen der Arbeitsstation des ViPNet-Administrators

Im ViPNet Netzwerkaufbau-Assistenten wurde eine neue Seite hinzugefügt, auf welcher der Typ des Netzwerkknotens für die Installation der Arbeitsstation des ViPNet Administrators ausgewählt werden kann.

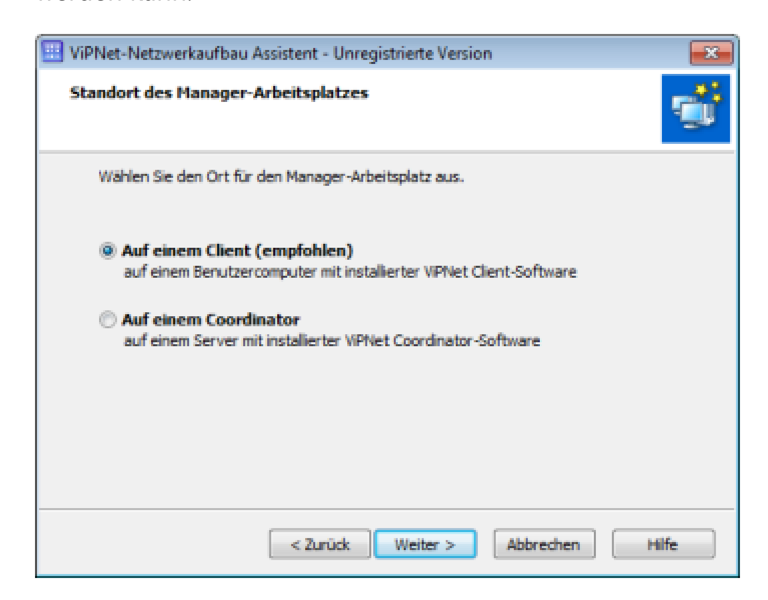


Abbildung 205. Standort des Manager-Arbeitsplatzes

- **Änderung der Benutzeroberfläche des Hauptfensters von ViPNet Network Manager**

  Damit für den Administrator die Arbeit mit Schlüsseln vereinfacht wird, wurde in der Symbolleiste die Schaltfläche **Schlüssel speichern** hinzugefügt. Bei Updates einer früheren Version von ViPNet Network Manager sollte diese Schaltfläche manuell der Symbolleiste des Programms hinzugefügt werden. Wählen Sie dazu in Menü Ansicht den Punkt **Symbolleiste anpassen**.

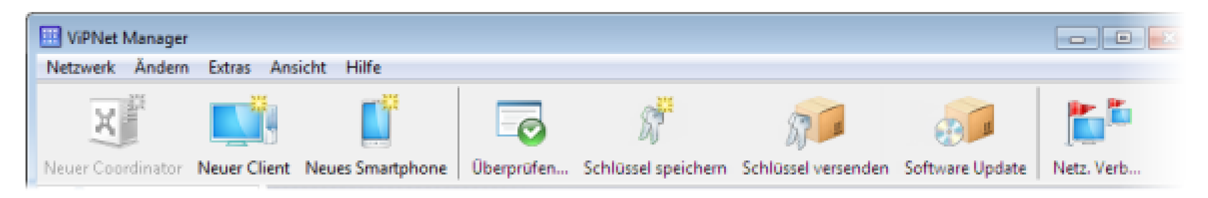


Abbildung 206. Symbolleiste des Programms ViPNet Manager

- **Verwendung des ViPNet Coordinator HW/VA-Coordinators als IPsec-Gateway**

  Es besteht nun die Möglichkeit, den ViPNet Coordinator HW/VA-Coordinator sowohl beim Einrichten von Verbindungen mit Smartphone-Clients, als auch bei Verbindungen zu einem anderen Netzwerk, in dem keine ViPNet Software eingesetzt wird, als IPsec-Gateway zu verwenden.

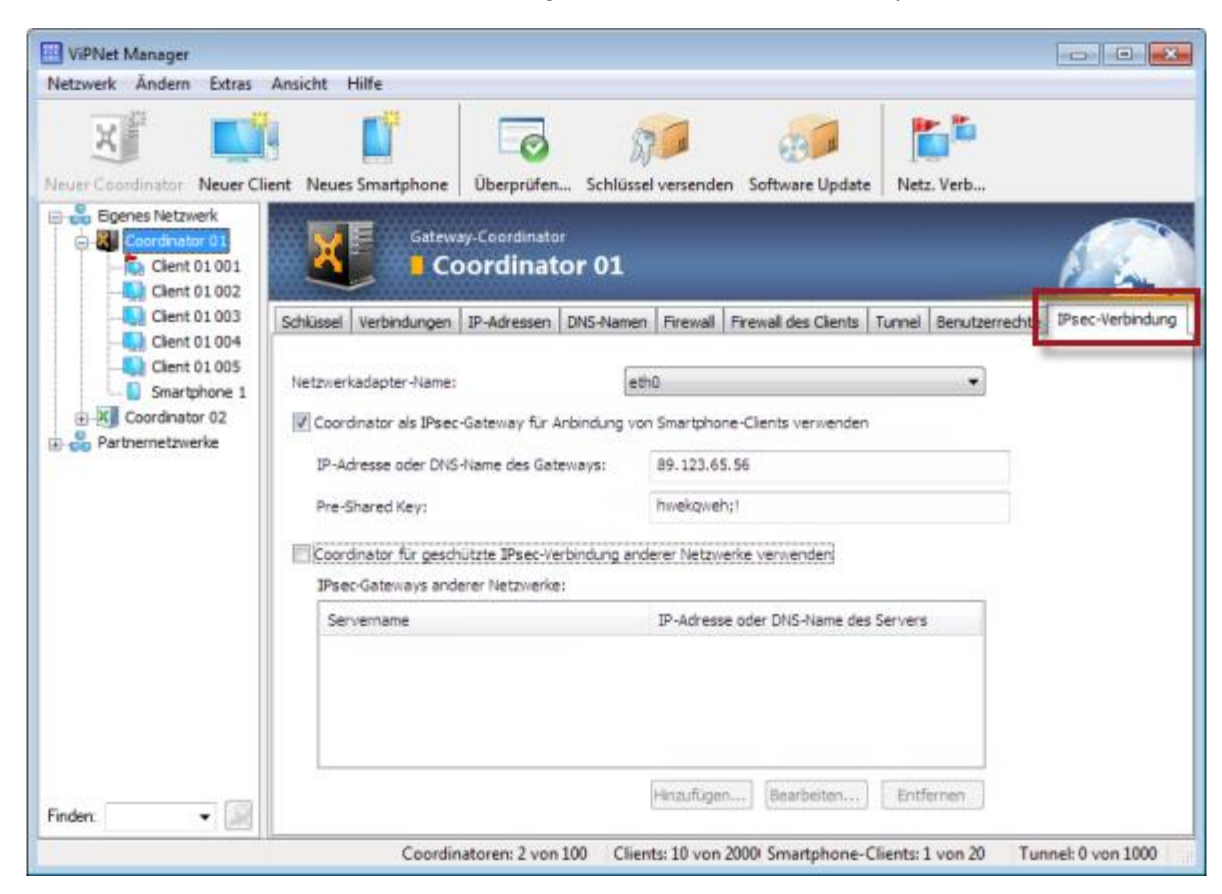


Abbildung 207. Verwendung des ViPNet Security Gateway-Coordinators als IPsec-Gateway

- **Erstellen von Konfigurationsdateien für den ViPNet Coordinator HW/VA-Coordinator**

  Beim Erstellen der Netzwerkknotenschlüssel für den ViPNet Coordinator HW/VA-Coordinator werden nun zusätzlich Konfigurationsdateien für die Installation der Schlüssel auf dem ViPNet Coordinator HW/VA-Coordinator sowie für eine mögliche Wiederherstellung der Standardeinstellungen der Software ViPNet Coordinator HW/VA erstellt. Dadurch kann die Software ViPNet Coordinator HW/VA durch Anschließen eines USB-Datenträgers mit der benötigten Datei an den Computer automatisch konfiguriert werden, ohne dass zusätzliche Schritte seitens des Benutzers erforderlich sind. Alle Konfigurationsparameter werden somit im Programm ViPNet Network Manager definiert.

- **Erfassen von Diagnoseinformationen beim Auftreten von Fehlern**

Während der Laufzeit von ViPNet Anwendungen werden nun im Hintergrund Daten über den Computer (Gesamtzustand des Systems, Soft- und Hardwareumgebung) und insbesondere über Ereignisse und Fehler im Betrieb der ViPNet Software gesammelt. Falls bei der Installation oder während der Laufzeit von ViPNet Anwendungen oder Microsoft SQL Server Störungen auftreten, wird vom System der Vorschlag angezeigt, eine Anfrage an den technischen Support der Firma „Infotecs" zu senden. Alle benötigten technischen Informationen werden dabei der Nachricht automatisch beigefügt.

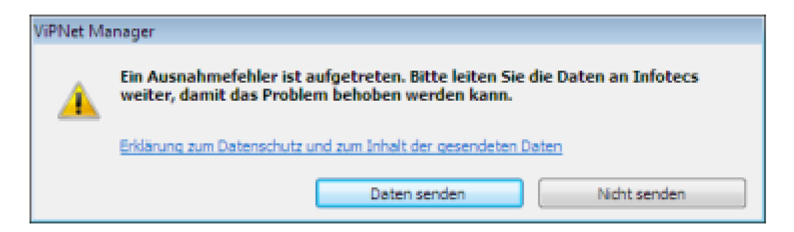


Abbildung 208. Fehler im Programm ViPNet Manager

Es werden keine vertraulichen Daten erfasst. Die Firma „Infotecs" nimmt den Schutz Ihrer persönlichen Daten sehr ernst und trifft alle erforderlichen Schutzmaßnahmen, um unberechtigte Zugriffe auf die erhaltenen Informationen oder eine unbefugte Weiterleitung der von Ihnen zur Verfügung gestellten Daten zu verhindern.

- **Kompatibilität mit dem Betriebssystem Microsoft Windows 8**

  Das Programm ViPNet Network Manager kann nun auf Computer installiert werden, die unter der Steuerung des Betriebssystems Windows 8 arbeiten.

- **Verwendung einer neuen Version von Microsoft SQL Server**

  Für die Speicherung der ViPNet Netzwerkparameter und der Programmeinstellungen von ViPNet Network Manager wird nun die Software Microsoft SQL Server 2008 R2 Express Edition verwendet, die mit dem Betriebssystem Windows 8 kompatibel ist. Die Installationsdatei von Microsoft SQL Server 2008 R2 Express Edition ist Bestandteil der Lieferung von ViPNet VPN.

- **Berechnung der verbleibenden Gültigkeitsdauer einer nicht registrierten Programmversion**

  In vorhergehenden Versionen von ViPNet Network Manager wurde die Berechnung der Gültigkeitsdauer einer nicht registrierten Programmversion immer ab dem Zeitpunkt der Installation durchgeführt. Nun erfolgt die Berechnung ab dem Zeitpunkt des ersten Programmstarts.

- **Erweiterte Möglichkeiten der nicht registrierten Version**

  In der nicht registrierten Version von ViPNet Network Manager gibt es nun folgende Möglichkeiten:

  - Es kann ein Smartphone-Client erstellt werden.
  - Es kann ein IPsec-Gateway verwendet werden.

  Außerdem kann neben einer nicht registrierten Version von ViPNet Network Manager zusätzlich das Programm ViPNet StateWatcher auf der Arbeitsstation des Administrators installiert werden. Das Programm ViPNet StateWatcher dient der Überwachung der Stati der ViPNet Netzwerkknoten, der Kontrolle der Sicherheitsereignisse auf den Knoten und der rechtzeitigen Erkennung von Störungen im Betrieb der Knoten samt unverzüglicher Benachrichtigung der Benutzer über die aufgetretenen Probleme.

- **Aktualisierung der Dokumentation und Hilfe**

Die Dokumentation und Hilfe von ViPNet VPN wurden aktualisiert. Es wurden Abschnitte hinzugefügt, die neue Möglichkeiten in der Funktionalität des Programms beschreiben.

Version 3.0.3

In diesem Abschnitt wird eine kurze Übersicht der Änderungen und neuen Möglichkeiten der Version 3.0.3 geboten.

- **Korrektur der Fehler**

  Fehler, die bei Verwendung vorheriger Programmversionen festgestellt wurden, wurden behoben

- **Aktualisierung der Dokumentation und Hilfe**

  Dokumentation und Hilfe von ViPNet VPN wurden ergänzt.

Version 3.0.2

In diesem Abschnitt wird eine kurze Übersicht der Änderungen und neuen Möglichkeiten der Version 3.0.2 geboten.

- **Automatischer Neustart bei Remoteinstallation der ViPNet Software**

  Im Installationsprogramm von ViPNet VPN besteht nun die Möglichkeit, bei Installation der Software ViPNet Client oder ViPNet Coordinator auf einem entfernten Computer einen automatischen Neustart dieses Computers durchzuführen. Dadurch können weitere Zugriffe auf den Remotecomputer zwecks Einleitung eines Neustarts vermieden werden.

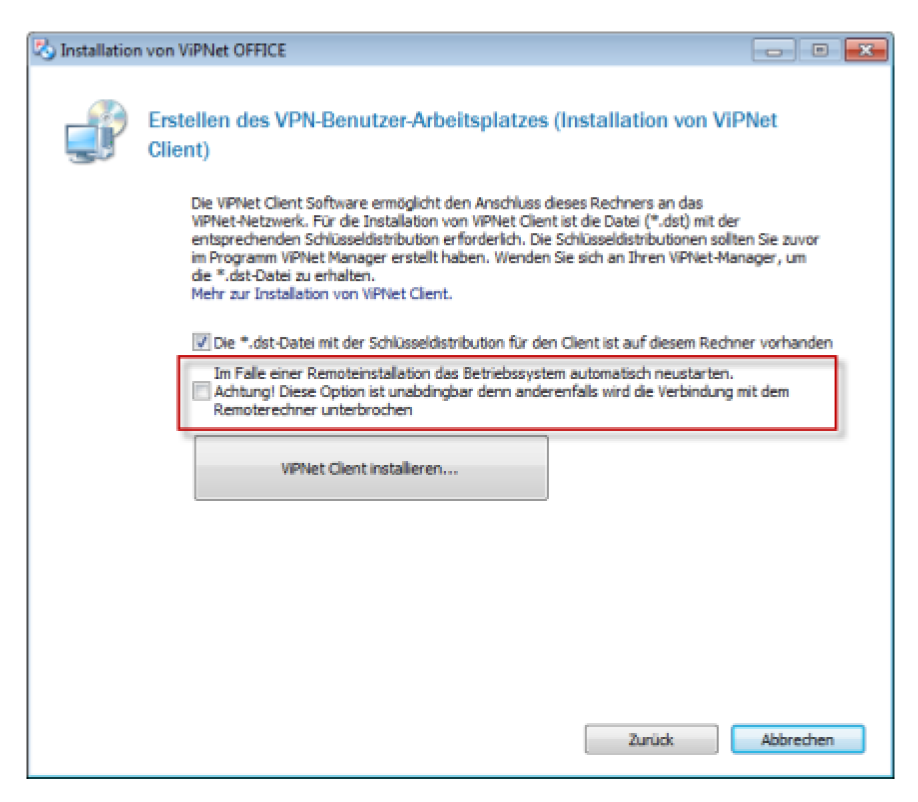


Abbildung 209. Die Möglichkeit, einen Remote-Computer neu zu starten

- **Aktualisierung der Dokumentation in französischer Sprache**

  Die französische Dokumentation und Hilfe von ViPNet VPN wurde grundlegend aktualisiert und entspricht nun vollständig der Dokumentation anderer Lokalisierungen.

Version 3.0.1

In diesem Abschnitt wird eine kurze Übersicht der Änderungen und neuen Möglichkeiten der Version 3.0.1 geboten.

- **Anbindung der Apple-Geräte iPad und iPhone an das ViPNet Netzwerk**

  Im Programm ViPNet Network Manager können nun Profile erstellt werden, mit deren Hilfe Verbindungen mobiler Apple-Geräte zum ViPNet Netzwerk bequem konfiguriert werden können. Die IPsec-Technologie gewährleistet einen geschützten Zugang mobiler Apple-Geräte zu ViPNet Netzwerkobjekten.

- **Verwendung des Programms ViPNet SafeDisk-V auf Clients**

  Es besteht nun die Möglichkeit zur Nutzung des Programms ViPNet SafeDisk-V auf Clients. Das Programm ist dazu bestimmt, vertrauliche Daten auf der Festplatte oder auf einem mobilen Datenträger zu schützen (s. ViPNet SafeDisk-V auf S. 40).

- **Veränderung der unterstützten Coordinator-Typen**

  Auf ViPNet Coordinatoren kann nun die Software ViPNet Coordinator HW/VA auf Basis des Betriebssystems Linux installiert werden. Auf Basis mehrerer Rechner mit installierter Software

ViPNet Coordinator für Windows kann jetzt mit Hilfe der Software ViPNet Cluster ein fehlertoleranter Cluster eingerichtet werden.

In Version 3.0 wird Hard- und Softwaresysteme ViPNet MiniGate nicht unterstützt.

- **Neue Vorgehensweise bei Aktualisierung der Netzwerkknotenschlüssel**

  Es genügt nun, bei einer Änderung von ViPNet Netzwerkstruktur oder Netzwerkknotenparametern den Befehl zum Versenden von Schlüsseln an die Netzwerkknoten oder zum Speichern der Schlüssel auf der Festplatte auszuführen. Schlüssel jener Knoten, deren Parameter sich geändert haben, werden dabei automatisch aktualisiert.

  In früheren Versionen von ViPNet Network Manager wurden Schlüssel immer in einem bestimmten Ordner abgelegt. Dadurch befanden sich jederzeit aktuelle Schlüsselversionen in diesem Ordner. Nun muss der Ordner für die Speicherung der Schlüsseldistribution jedesmal separat ausgewählt werden. Die Schlüssel in diesem Ordner gelten nur zum Zeitpunkt der Speicherung als aktuell und werden nicht mehr automatisch aktualisiert.

- **Export und Import der ViPNet Network Manager-Konfiguration**

  Es besteht die Möglichkeit, eine ViPNet Network Manager-Konfiguration mitsamt aller Programmeinstellungen und ViPNet Netzwerkparameter in eine Datei zu exportieren oder aus einer Datei zu importieren. Diese Funktion ermöglicht es, die Software ViPNet Network Manager mitsamt aller Daten auf einen anderen Computer zu übertragen oder das Programm im Fall einer Störung wiederherzustellen.

- **Gemeinsames Administratorpasswort für alle Netzwerkknoten**

  Auf allen Netzwerkknoten wird nun für den Zugang zu zusätzlichen Funktionen und Einstellungen des Programms ViPNet Monitor ein gemeinsames Administratorpasswort verwendet.

- **Verdeckte Darstellung der Benutzerpasswörter**

  In der Registerkarte **Schlüssel** werden nun Benutzerpasswörter und Passwortphrasen standardmäßig verdeckt dargestellt. Passworteigenschaften können im Fenster **Einstellungen** in der Registerkarte **Benutzer-Passwörter** verändert werden.

- **Änderung der grafischen Benutzeroberfläche im Programm ViPNet Network Manager**

  Die grafische Benutzeroberfläche des Programms ViPNet Network Manager wurde wesentlich überarbeitet; sie ist nun benutzerfreundlicher und attraktiver gestaltet.



Abbildung 210. Änderungen der Benutzeroberfläche des ViPNet Manager 3.0

- **Neue Datenbankstruktur im Programm ViPNet Network Manager**

  Für die Speicherung von Struktur und Parametern des geschützten Netzwerks sowie von Programmeinstellungen wird nun das Datenbanksystem Microsoft SQL Express 2005 benutzt. Auf diese Weise wurden die Verwendungsmöglichkeiten von ViPNet Network Manager bei der Arbeit mit großen Netzwerken erweitert.

- **Geänderte Möglichkeiten der Programme ViPNet Client und ViPNet Coordinator**

  Das Paket ViPNet VPN 3.0 beinhaltet die Programme ViPNet Client und ViPNet Coordinator der Version 3.2. Ausführliche Informationen über mögliche Änderungen und Verbesserungen in diesen Programmen finden Sie in der entsprechenden Dokumentation (Hilfe).

- **Ergänzung der ViPNet VPN Dokumentation**

  Im Lieferumfang sind nun folgende Dokumente inkludiert: „ViPNet VPN. Schnellstart“, „Verbreitete Szenarien bei der Administration von ViPNet VPN. Anhang zum Benutzerhandbuch“, „Die Technologie von ViPNet. Allgemeine Informationen.“, „Grundsätze beim Aufbau von Verbindungen im ViPNet Netzwerk. Allgemeine Informationen“.

Version 2.2

In diesem Abschnitt wird eine kurze Übersicht der Änderungen und neuen Möglichkeiten der Version 2.2 geboten.

- **Erweiterte Möglichkeiten von Partnernetzwerk-Verbindungen**

  Es besteht jetzt die Möglichkeit, Partnernetzwerk-Verbindungen für Netzwerke herzustellen, die mit Hilfe des Pakets ViPNet VPN auf der einen Seite, und ViPNet CUSTOM auf der anderen Seite erstellt wurden.

- **Speicherung des Benutzerpassworts in der Registry**

  Im ViPNet Network Manager kann das Speichern des Passwortes jedes Benutzers erlaubt oder verboten werden.



Abbildung 211. Speichern des Benutzerpassworts konfigurieren

- **Unterstützung von Siemens CardOS Smartcards**

  Siemens CardOS Smartcard wird jetzt unterstützt und kann als zusätzlicher Faktor für die Authentisierung verwendet werden.

- **Dokumentation und Hilfe in anderen Sprachen**

  Es wurden die Dokumentation und die Hilfe für ViPNet VPN Produkte auf Französisch und die Hilfe auf Deutsch herausgegeben.

Version 2.1

In diesem Abschnitt wird eine kurze Übersicht der Änderungen und neuen Möglichkeiten der Version 2.1 geboten.

- **Vereinfachte Vorgehensweise bei der Erstinstallation des Netzwerks**

  Mit ViPNet VPN 2.1 können Sie bereits bei der Erstellung der Netzwerkstruktur die Verbindung zwischen der Arbeitsstation mit der Software ViPNet Network Manager (Administrator-Arbeitsplatz)

und ihrem Coordinator konfigurieren. Der Zeitaufwand für die Konfiguration der Netzwerkknoten wird dadurch erheblich gesenkt.

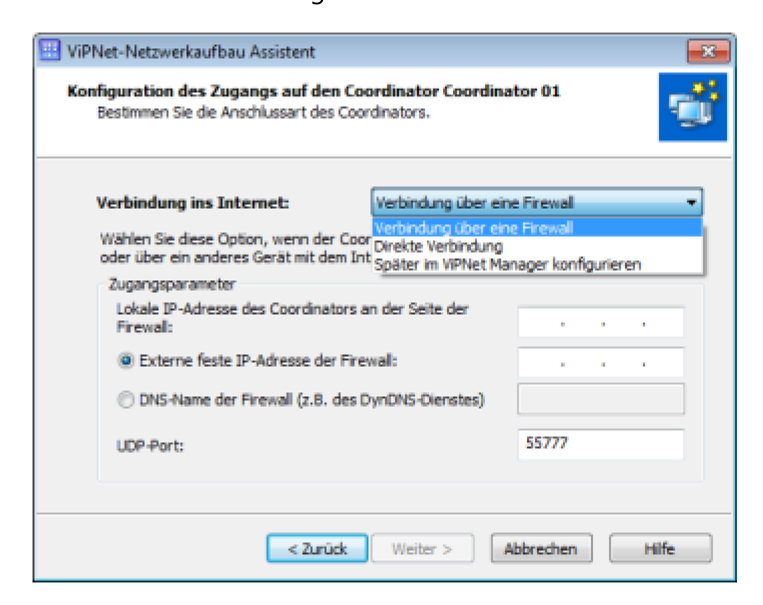


Abbildung 212. Einstellung des Zugangs zum Coordinator während der Netzwerkinstallation

- **Wahl des Coordinatortyps für die Weiterleitung von Aktualisieren**

  Es besteht die Möglichkeit zur Angabe des Coordinatortyps für die spätere Weiterleitung von Software-Aktualisieren des entsprechenden Typs an diesen Coordinator. Auf diese Art können innerhalb des ViPNet Netzwerks Coordinatoren mit unterschiedlichen Betriebssystemen (Windows, Linux, etc.) sowie Coordinatoren auf Basis unterschiedlicher integrierter Lösungen (Hard- und Softwaresysteme ViPNet MiniGate) verwendet werden.



Abbildung 213. Coordinatortyp angeben

- **Erhöhte Anzahl unterstützter Betriebssysteme**

  Betriebssysteme Vista (64 Bit)/Server 2008 (32/64 Bit)/Windows 7 (32/64 Bit) werden unterstützt.

Version 2.0

In diesem Abschnitt wird eine kurze Übersicht der Änderungen und neuen Möglichkeiten der Version 2.0 geboten.

- **Partnernetzwerk-Verbindungen**

  Es besteht die Möglichkeit zur Herstellung von Partnernetzwerk-Verbindungen. Eine Partnernetzwerk-Verbindung bedeutet, dass zwischen zwei vertrauenswürdigen ViPNet Netzwerken eine geschützte Verbindung organisiert werden kann. Für die Konfiguration der Partnernetzwerk-Verbindung wird ein komfortabler Assistent benutzt, mit dessen Hilfe alle notwendigen Einstellungen ohne spezielles Hintergrundwissen und ohne Verwendung zusätzlicher Dokumentation vorgenommen werden können.

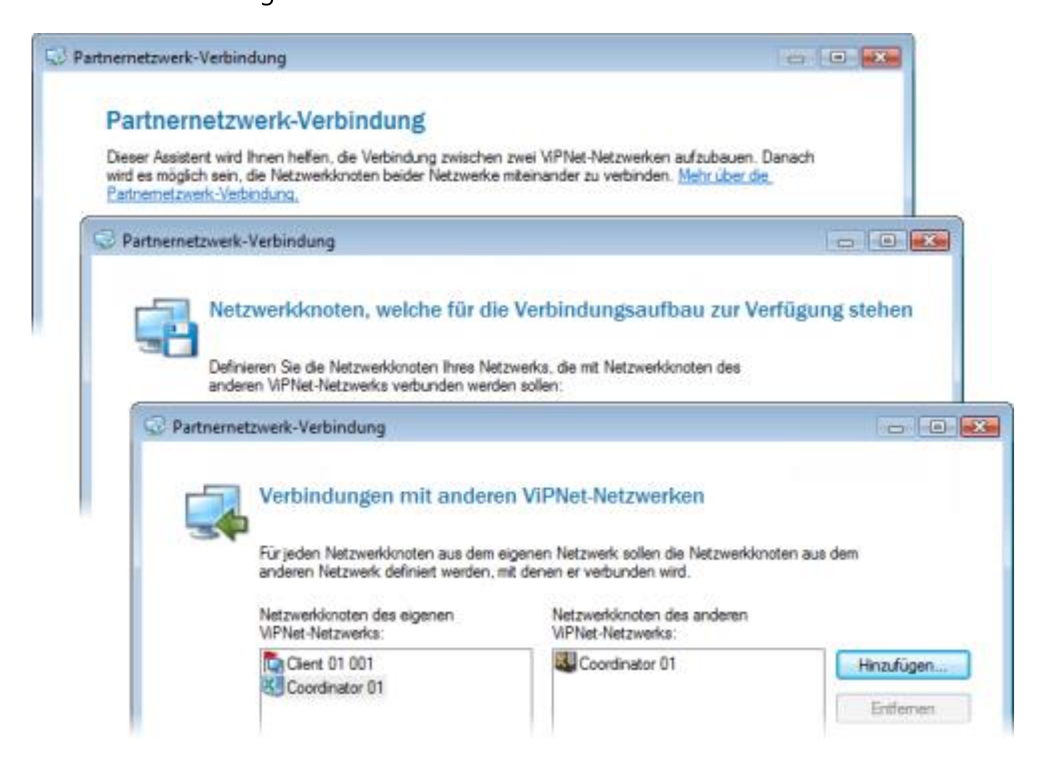


Abbildung 214. Einige Seiten des Partnernetzwerk-Assistenten

- **Modifikation von Verbindungen zwischen Coordinatoren**

  Sie können die Verbindungen zwischen den Coordinatoren konfigurieren. Die obligatorischen Verbindungen mit dem Coordinator, dem die Arbeitsstation des ViPNet Administrators zugeordnet ist, können weiterhin nicht gelöscht werden. Dies soll helfen, Fehler beim Editieren zu vermeiden, um die Funktionsfähigkeit des ViPNet Netzwerks nicht zu gefährden.

- **Definition der Benutzerrechte für ViPNet Benutzer**

  Sie können Benutzerrechte für einzelne ViPNet Netzwerkknoten vergeben. Bestimmte Einstellungen können blockiert und vom Benutzer nicht mehr geändert werden. Außerdem können bestimmte Elemente der grafischen Benutzeroberfläche deaktiviert werden. Dies erhöht die Sicherheit und Zuverlässigkeit eines ViPNet Netzwerks.



Abbildung 215. Benutzerrechte definieren



Externe Datenträger

Allgemeine Informationen

Externe Geräte werden zum Speichern der Schlüsselcontainer (auf S. 372) verwendet. Diese Schlüsselcontainer können für die Authentifizierung, zum Erstellen von digitalen Signaturen oder für andere Zwecke verwendet werden.

Auf dem externen Gerät können Schlüssel gespeichert werden, die mit Hilfe unterschiedlicher Algorithmen in ViPNet Software oder in Drittanwendungen erstellt wurden. Die maximale Anzahl der Schlüsselcontainer, die auf einem externen Gerät gespeichert werden können, hängt von der Speicherkapazität des Geräts ab.

Die Software ViPNet Network Manager unterstützt zwei Arten der Authentifizierung mit Hilfe eines externen Geräts (s. Authentisierungsmodi auf S. 335):

- Mit dem privaten Schlüssel des ViPNet Benutzers, der auf dem Gerät gespeichert wird. Diese Art der Authentifizierung hat die folgenden Einschränkungen:
    - Ein externes Gerät kann nicht für die Authentifizierung mehrerer ViPNet Benutzer verwendet werden.
    - Ein externes Gerät kann nicht für die Authentifizierung eines Benutzers auf mehreren ViPNet Knoten verwendet werden.
    - Wenn diese Art der Authentifizierung verwendet wird, dann müssen die Signaturschlüssel des Benutzers, die mit Hilfe von ViPNet Software in der Zertifizierungsstelle erstellt wurden, auf dem gleichen Gerät wie der private Schlüssel gespeichert sein.
- Mittels Zertifikat, das gemeinsam mit dem entsprechenden privaten Schlüssel auf dem Gerät gespeichert wird.

Das Zertifikat für die Authentifizierung kann in der Windows-Domäne angefordert werden. Der Schlüsselcontainer wird dabei auf einem externen Gerät gespeichert, das den Standard PKCS#11 unterstützt.

Alle Operationen mit Schlüsselcontainern und externen Geräten können Sie im Programm ViPNet CSP durchführen. Damit ein externes Gerät auf dem Computer verwendet werden kann, sollten zunächst die Treiber dieses Geräts installiert werden. Stellen Sie vor dem Speichern der Schlüssel auf dem Gerät sicher, dass das Gerät formatiert ist.

Liste externer Datenträger

In der nachfolgenden Tabelle sind externe Geräte aufgelistet, die im Programm ViPNet Network Manager verwendet werden können. Für jedes externe Geräte werden die Beschreibung, die Bedingungen und Besonderheit der Verwendung sowie Informationen zur Unterstützung des Standards PKCS#11 aufgeführt.

Tabelle 17. Liste externer Datenträger

Name des Geräts in Software ViPNet CSP	Vollständiger Name und Gerätetyp	Anwendungsbedingungen	Unterstützung von PKCS#11
eToken Aladdin	Persönlicher elektronischer Schlüssel **eToken PRO (Java)**, **eToken PRO** vom Hersteller Aladdin.	Auf dem Netzwerkknoten muss die Software PKI Client 5.1 oder höher installiert sein. eToken PRO SmartCard kann mit jedem PC/SC-kompatiblen Smart Card Reader benutzt werden.	Ja
iButton Aladdin	Elektronischer Schlüssel **Dallas**, **iButton** Typ **DS1993**, **DS1994**, **DS1995** und **DS1996**.	Das Lesegerät muss an den Computer angeschlossen werden. Auf dem Computer muss die Software zur Datenübertragung mit iButton, 1-Wire Drivers Version 3.20 oder Version 4.0.3 installiert sein. In den Betriebssystemen Windows XP und Server 2003 kann neben ViPNet Software ausschließlich die Software 1-Wire Drivers Version 3.20 verwendet werden.	Nein
Smartcard Athena	Karten mit dem Speichertyp I2C (ASE M4), synchrone Karten mit dem Bustyp 2/3 und geschütztem Speicher nach ISO7816-3 (ASE MP42).	Das Auslesen und Eintragen der Daten auf Smartcard erfolgt durch den CardReader ASEDrive III PRO-S des Herstellers Athena. Die Treiber der Version 2.6 sollen auf dem PC installiert werden.	Nein

Name des Geräts in Software ViPNet CSP	Vollständiger Name und Gerätetyp	Anwendungsbedingungen	Unterstützung von PKCS#11
Siemens CardOS	SmartCards **CardOS/M4.01a, CardOS V4.3B**, **CardOS V4.2B**, **CardOS V4.2B DI**, **CardOS V4.2C**, **CardOS V4.4** vom Hersteller Atos (Siemens).	Auf dem Computer muss die Software Siemens CardOS API V5.0 oder höher installiert werden.	Ja



Glossar

A

Aktualisieren der Schlüsseldistributionen

Die Netzwerkknotenschlüssel werden durch den Administrator des ViPNet Network Managers durchgeführt. Im Zuge verschiedener Veränderungen an der logischen Struktur des Netzwerkes (Löschen oder Erstellen der Netzwerkknoten, Definieren neuer Verbindungen) verändern sich auch die Adresslisten und Schlüssel für die betroffenen Netzwerkknoten. Der Administrator des ViPNet Network Managers erstellt und versendet die aktuellen Schlüsseldistributionen.

B

Benutzerpasswort

Persönliches Passwort des Benutzers für die Anmeldung an seinem ViPNet Netzwerkknoten. Ursprünglich wird das Passwort im ViPNet Network Manager (in ViPNet VPN-Netzwerke) oder ViPNet Network Control Center (in ViPNet Netzwerke basierte auf der Software ViPNet Administrator) erstellt, kann aber durch den Benutzer geändert werden.

C

Client

Netzwerkknoten, der entweder einen Ausgangs- oder Endpunkt für die Datenübertragung darstellt. Im Vergleich mit dem Coordinator verfügt der Client über keine Routing-Funktionen.

Container-Datei

Eine Datei, welche die geschützten Daten beinhaltet. Diese Datei wird als ein Laufwerk unter Windows angezeigt. Sie können mit ihr wie mit einem Laufwerk arbeiten und dort Dateien speichern, kopieren, einfügen, verschieben, löschen u. s. w.

Eine Containerdatei hat die Dateierweiterung *.sdc und ist standardmäßig ausgeblendet. Um diese Datei anzusehen wählen Sie in der Windows-Explorer Menüleiste unter **Extras** den Menüpunkt **Ordner- und Suchoptionen** und auf der Registerkarte **Ansicht** deaktivieren Sie die Option **Geschützte Dateien ausblenden (empfohlen)**.

Coordinator (ViPNet Coordinator)

Ein Netzwerkknoten, auf dem die Software ViPNet Coordinator oder ViPNet Coordinator HW installiert ist. Ein ViPNet Coordinator funktioniert als ein Server innerhalb des ViPNet Netzwerks und leitet VPN-Traffic und Systemdaten weiter.

D

Datei (Transportdatei)

Dienstinformation, die innerhalb des ViPNet Netzwerkes verwendet wird und durch das MFTP-Modul übermittelt wird.

DHCP-Dienst (Dynamic Host Configuration-Protokoll)

Das Dynamic Host Configuration Protocol (DHCP) ermöglicht die automatisierte Zuweisung der Netzwerkkonfiguration an die Clients durch einen Server.

E

Externe IP-Adressen

Die Adressen eines externen Netzwerkes.

Externes Netzwerk

Das Netzwerk mit einem anderen IP-Adressen-Bereich im Vergleich mit dem lokalen Netzwerk. Normalerweise wird dieser Begriff für das Internet verwendet.

G

Gateway-Coordinator

Der Coordinator, der für die Verbindungen zwischen den vertrauten Netzwerken verantwortlich ist. Wird im ViPNet Network Manager beim Aufbau der Verbindung mit einem vertrauten Netzwerk definiert.

Geschützte Verbindung

Eine verschlüsselte Verbindung zwischen ViPNet Netzwerkknoten.

Geschützter DNS- oder WINS-Server

Ein DNS- oder WINS-Server, installiert auf einem ViPNet Netzwerkknoten.

Geschützter Netzwerkknoten

Computer mit installierter ViPNet Software.

Getunneltes Objekt

Ein Netzwerkobjekt, das über keine ViPNet Client – bzw. Coordinator Software verfügt und durch einen Coordinator getunnelt wird.

I

Internetzwerk-Masterschlüssel

Ein Masterschlüssel, der für das Generieren anderer Schlüssel verwendet wird, die ihrerseits für die Kommunikation zwischen den Partner-Netzwerken eingesetzt werden.

N

Netzwerkadressenübersetzung (NAT)

Network Address Translation ist der Sammelbegriff für Verfahren, die automatisiert Adressinformationen in Datenpaketen durch andere ersetzen, um verschiedene Netze zu verbinden.

Netzwerkfilter

Eine Zusammensetzung von Parametern, auf deren Basis die Firewall der ViPNet Software bestimmte IP-Pakete blockiert oder erlaubt.

Netzwerkknotenadministrator-Passwort

Das Passwort für die Anmeldung auf einem ViPNet Netzwerkknoten im Administratormodus. In diesem Modus stehen zusätzliche Konfigurationsmöglichkeiten für ViPNet Anwendungen zur Verfügung. Das Passwort des ViPNet Netzwerkknotenadministrators kann vom Administrator des ViPNet Netzwerks im Programm ViPNet Key and Certification Authority (ViPNet Netzwerke basierte auf der Software ViPNet Administrator) bzw. ViPNet Network Manager (ViPNet VPN-Netzwerke) erstellt werden.

O

Offener DNS- oder WINS-Server

DNS- oder WINS-Server auf einem ungeschützten Computer.

Offener Netzwerkknoten

Ein Netzwerkobjekt ohne ViPNet Software.

Öffentliche IP-Adressen

Alle IP-Adressen, die nicht für die privaten Bereiche reserviert sind.

P

Partnernetzwerk

Ein vertrautes ViPNet Netzwerk, das mit dem eigenen ViPNet Netzwerk verbunden ist.

Partnernetzwerk-Information

Die Partnernetzwerk-Information dient zum Aufbau oder der Veränderung von Partnernetzwerkverbindungen.

Private IP-Adresse

Private IP-Adressen gehören zu bestimmten IP-Adressbereichen, die im Internet nicht geroutet werden. Sie können von jedem für private Netze wie etwa LANs verwendet werden und umfassen die Bereiche 10.0.0.0-10.255.255.255; 172.16.0.0-172.31.255.255; 192.168.0.0-192.168.255.255.

S

Schlüsselcontainer

Datei, in der der private Schlüssel und das zugehörige Zertifikat des öffentlichen Schlüssels gespeichert sind. Beim Bilden einer Anfrage für die Zertifikatsaktualisierung wird der Name des Containers, in dem das neue Schlüsselpaar der Signatur (privater Schlüssel und das Zertifikat) aufbewahrt wird, automatisch vergeben und hat die Form `sgn-<Zufallszahl im Hexadezimalformat>`.

Schlüsseldistribution

Die Datei mit der Erweiterung `.dst`, wird im ViPNet Network Manager (in ViPNet VPN-Netzwerke) oder ViPNet Network Control Center (in ViPNet Netzwerke basierte auf der Software ViPNet Administrator) erstellt. Die Datei beinhaltet Schlüsselinformationen, Adresslisten und die Lizenzdatei, die für den initialen Start des Netzwerkknotens erforderlich sind.

Schutzschlüssel

Schlüssel, mit Hilfe von dem andere Schlüssel verschlüsselt wird.

Sichtbare Adressen

IP-Adressen, virtuelle oder reelle, unter denen der Netzwerkknoten für alle anderen sichtbar ist.

T

Terminal (Terminalclient)

Computer, der für den Zugang zu Anwendungen und Daten, die sich auf dem Terminalserver befinden, verwendet wird.

Tunnelung

Verschlüsselung des Traffics der offenen Netzwerkobjekte bei der Übertragung über öffentliche Netzwerke.

V

ViPNet Benutzer

Der im ViPNet Network Manager erstellte Benutzer. Für ihn werden die Schlüsseldistribution und das Benutzer-Passwort generiert.

ViPNet Network Manager Administrator

Person, die über den Zugriff auf das ViPNet Network Manager verfügt und für die Konfiguration des ViPNet Netzwerkes sowie das Erstellen der Schlüsselinformationen verantwortlich ist.

ViPNet Network Manager Administratorpasswort

Das Passwort für die Anmeldung am ViPNet Network Manager.

ViPNet Netzwerkknoten

Computer mit installierter ViPNet Software.

ViPNet VPN Lizenz

Die Lizenz bestimmt die Netzwerknummer, die Anzahl der Netzwerkknoten für bestimmte Anwendungen und Einzelkomponenten der ViPNet Produkte, die maximal erlaubte Version der Software, die Laufzeit der Software und andere Parameter.

Virtuelles Privates Netzwerk (VPN)

Das konventionelle VPN dient dazu, Teilnehmer eines Netzes (auch mobile Benutzer) aus ihrem ursprünglichen Netz heraus an ein anderes Netz anzubinden. Diese Anbindung erfolgt üblicherweise über öffentliche Netze unter Verwendung von Verschlüsselungs- und Authentisierungsmechanismen.



Index

A

C

D

I

L

N

S

T

U

V

W